د لوړو زده کړو وزارت
د کابل پوهنتون
علمي معاونيت
د حقوقو او سياسي علومو پوهنځی
د سياسي علومو او نړيوالو اړيکو ډيپارټمنټ

پر ملی امنیت د مصنوعي ځیرکتیا اغیزې

(د لیسانس د دورې پایلیک)

څېړونکي: اسدالله عزیزی کاکړ
لارښود استاد: شمس الرحمن رحمانزی
تحصيلي کال: ۱۴۰۵ هـ . ل

ډالـــۍ

زه دا اثر په ډېر درناوي او ژورې مینې سره خپلو ګرانو کورنۍ ته ډالۍ کوم؛ هغو مهربانو او قدرمنو انسانانو ته چې د ژوند په ټولو پړاوونو کې یې زما ملاتړ کړی او تل یې زما لپاره د مینې، مهربانۍ او پناه سیوری غوړولی دی. زه به د دوی د بې‌شمېره زحمتونو، ستړیاوو او قربانیو مننه‌وی پاتې شم. ګرانو والدینو! تاسو زما د زده‌کړې په بهیر کې همېشه د هڅونې، لارښوونې او ملاتړ مهمه سرچینه پاتې شوي یاست او زما د بریالیتوب لپاره مو بنسټیز رول ترسره کړی دی. هیله لرم چې ستاسو د هیلو وړ خدمتګار وګرځم او تاسو، خپلې ټولنې او خپل هېواد ته ګټور واوسم. همدارنګه، تمه لرم چې اوس او په راتلونکې کې ستاسو لپاره د ویاړ لامل وګرځم.

دوهم، دا اثر خپلو درنو او قدرمنو ښوونکو ته ډالۍ کوم؛ هغو استادانو ته چې د علم او پوهې په لار کې یې د ورځې او شپې نه ستړې کېدونکې هڅې کړې دي. زه د هغوی د زحمتونو، لارښوونو او علمي خدمتونو څخه ژوره مننه کوم، ځکه چې د هغوی هڅو زما د علمي او فکري ودې بنسټونه پیاوړي کړي دي.

درېیم، دا اثر خپلو ټولو ګرانو ملګرو، خپلوانو او د علم، پوهې او رڼا ټولو مینه‌والو ته ډالۍ کوم، چې په بېلابېلو بڼو یې زما ملاتړ کړی او زما د بریالیتوب په لاره کې یې راسره مرسته کړې ده.

په پای کې، له پاک څښتن تعالی څخه په ډېر اخلاص هیله کوم چې موږ او تاسو ټولو ته د ژوند په هر پړاو کې د بریا، توفیق او نېکمرغۍ لارې هواري کړي، زموږ هڅو ته اجر او برکت وبښي او موږ د خپلو موخو د ترلاسه کولو جوګه وګرځوي.

لنډيزه

په دې څېړنه کې د نويو ټکنالوژيو، په ځانګړي ډول د مصنوعي ځيرکتيا، پر ملي امنيت د اغېزو هراړخيزه ارزونه شوې ده. په معاصر نړيوال چاپېريال کې د ټکنالوژۍ چټک پرمختګ د دولتونو دوديز امنيتي جوړښتونه له بنسټيزو بدلونونو او نويو ننګونو سره مخ کړي دي، چې له امله يې د ملي امنيت مفهوم پراخ شوی او نوې بڼې يې خپلې کړې دي.دا څېړنه هڅه کوي وښيي چې مصنوعي ځيرکتيا او نورې نوې ټکنالوژۍ د ملي امنيت په بېلابېلو ابعادو لکه سياسي، پوځي، اقتصادي، سايبري او ټولنيزو برخو کې څه ډول اغېز لري. په همدې موخه، د مصنوعي ځيرکتيا ونډه د معلوماتو د شننې، استخباراتي فعاليتونو، پوځي تګلارو، اقتصادي سيالۍ او سايبري امنيت په چوکاټ کې ارزول شوې ده.دغه څېړنه د توصيفي–تحليلي کړنلارې له مخې ترسره شوې ده او په کې له کتابتوني سرچينو لکه علمي کتابونو، څېړنيزو مقالو او نړيوالو راپورونو څخه ګټه اخيستل شوې ده. راټول شوي معلومات په کيفي بڼه شنل شوي او د بېلابېلو ليکوالانو نظريات پرتله او ارزول شوي دي.د څېړنې موندنې ښيي چې مصنوعي ځيرکتيا د ملي امنيت لپاره هم فرصتونه او هم ګواښونه رامنځته کوي. له يوې خوا، دا ټکنالوژي د پرېکړې کولو بهير چټکوي، د معلوماتو شننه دقيقوي او د امنيتي بنسټونو وړتياوې پياوړې کوي؛ خو له بلې خوا، د سايبري بريدونو، معلوماتي جګړو، د شخصي محرميت د نقض او د خودکارو وسلو د پراختيا له امله نوي امنيتي ګواښونه هم راولاړوي.په پای کې، څېړنه سپارښتنه کوي چې د مصنوعي ځيرکتيا د اغېزمنې او خوندي کارونې لپاره بايد روښانه پاليسۍ، قانوني چوکاټونه او تخنيکي کنټرولونه رامنځته شي، څو د دې ټکنالوژۍ له فرصتونو اعظمي ګټه واخيستل شي او احتمالي ګواښونه يې راکم کړل شي.

کليدي کلمې: مصنوعي ځيرکتيا، ملي امنيت، نوې ټکنالوژۍ، سايبري امنيت، پوځي تګلارې، معلوماتي جګړه، امنيتي پاليسۍ

لیک لړ

سریزه

ټکنالوژي د معاصرې زمانې له مهمو او اغېزناکو پدیدو څخه ده چې د نړیوال نظام په جوړښت، د دولتونو په اړیکو او د نړیوالو لوبغاړو په تعاملاتو کې یې ژور بدلونونه رامنځته کړي دي. له همدې بدلونونو سره، د نړیوالو اړیکو یو اساسي مفهوم، یعنې امنیت، هم له نویو ننګونو او بدلونونو سره مخ شوی دی. امنیت له پخوا راهیسې د انسانانو، دولتونو او نړیوالو بنسټونو د پاملرنې وړ موضوع پاتې شوې ده، خو په معاصر پېر کې یې ابعاد لا پراخ شوي دي. د نړیوالو اړیکو بېلابېلو نظریو امنیت ته له بېلابېلو لیدلورو کتنه کړې ده. ریالیستانو تر ډېره د امنیت پر مادي او پوځي اړخ ټینګار کړی، په داسې حال کې چې لیبرالیستانو د امنیت غیرپوځي اړخونه لکه اقتصادي او ټولنیز ابعاد هم مهم بللي دي. له بلې خوا، سازهانګارانو د امنیت مفهوم د ټولنیزو او هنجاري جوړښتونو په رڼا کې بیا تفسیر کړی دی.په معاصر پېر کې د نویو ټکنالوژیو، په ځانګړي ډول د مصنوعي ځیرکتیا، چټک پرمختګ د انسان د ژوند په بېلابېلو برخو کې ژور بدلونونه رامنځته کړي دي. مصنوعي ځیرکتیا د معلوماتو د شننې، پرېکړهنیونې، سایبري فعالیتونو او پوځي چارو په برخه کې مهم رول لوبوي. دا ټکنالوژي د نورو پرمختللو سیستمونو لکه د شیانو انټرنېټ او لویو معلوماتو سره په یوځای کېدو لا اغېزمنه شوې او د نړیوالو لوبغاړو پاملرنه یې ځانته را اړولېده.له دې سره، دا پوښتنه راپورته کېږي چې مصنوعي ځیرکتیا د دولتونو پر ملي امنیت څه ډول اغېز لري. دا ټکنالوژي، چې ماشینونو ته د معلوماتو د درک او تحلیل وړتیا ورکوي، کولی شي هم د امنیت د پیاوړتیا وسیله وګرځي او هم نوي ګواښونه رامنځته کړي، لکه سایبري بریدونه، معلوماتي جګړې او د خودکارو وسلو پراختیا.دا څېړنه پر دې بنسټ ولاړه ده چې مصنوعي ځیرکتیا نه یوازې یو فرصت دی او نه هم یوازې یو ګواښ، بلکې دواړه اړخونه لري. د دې ټکنالوژۍ اغېزې د دولتونو د پالیسۍ او کارونې له څرنګوالي سره تړاو لري. له همدې امله، په دې څېړنه کې هڅه شوې ده چې د مصنوعي ځیرکتیا د اغېزو ارزونه وشي او د هغو هېوادونو د تجربو له مخې، چې په دې برخه کې پرمختللي دي، د ملي امنیت پر بېلابېلو ابعادو یې اغېزې وڅېړل شي.په ټوله کې، د نویو ټکنالوژیو، په ځانګړي ډول د مصنوعي ځیرکتیا، چټک پرمختګ د ملي امنیت مفهوم له نویو ننګونو او فرصتونو سره مخ کړی، چې څېړنه یې د معاصرې نړۍ یو مهم علمي او عملي ضرورت ګڼل کېږي.

د څېړنې جوړښت

د ستونزې بيان

ملي امنيت د هر دولت له اساسي او حياتي لومړيتوبونو څخه شمېرل کېږي، ځکه چې د دولت بقا، سياسي ثبات، اقتصادي پرمختګ او ټولنيز نظم تر ډېره له همدې مفهوم سره تړلي دي. د نړيوالو اړيکو په دوديزو نظريو کې ملي امنيت زياتره د پوځي ځواک، جغرافيايي بشپړتيا او د بهرنيو ګواښونو پر وړاندې د دولت د دفاعي وړتيا له مخې تعريف شوی دی. خو په معاصر نړيوال نظام کې دغه دوديز تعريف د نويو ټکنالوژيو، په ځانګړې ډول مصنوعي ځيرکتيا، د پراختيا له امله له ژورو بدلونونو سره مخ شوی دی.

په وروستيو لسيزو کې د معلوماتي او ډيجيټل انقلاب په پايله کې داسې ټکنالوژۍ رامنځته شوې چې نه يوازې د انسان د ژوند بڼه يې بدله کړې، بلکې د دولتونو د ځواک جوړښت، امنيتي پاليسۍ او د ګواښونو ماهيت يې هم له سره تعريف کړی دی. مصنوعي ځيرکتيا د همدې بدلونونو له مهمو او اغېزناکو ټکنالوژيو څخه ده، چې کولای شي په خپلواکه يا نيمه‌خپلواکه ډول معلومات تحليل کړي، تصميم ونيسي او پيچلي امنيتي او تخنيکي دندې ترسره کړي.

د مصنوعي ځيرکتيا د پراخېدو سره، د ملي امنيت دوديزې لارې چارې له نويو فرصتونو او همدارنګه له جدي ننګونو سره مخ شوې دي. له يوې خوا، دا ټکنالوژي د دولتونو د دفاعي سيستمونو، استخباراتي تحليلونو، د ګواښونو د وړاندوينې او د پربکړه‌نيونې په چټکتيا او دقيقوالي کې مهم پرمختګونه رامنځته کوي. د بېلګې په توګه، د لويو معلوماتو تحليل او د اتوماتيکو سيستمونو کارول کولای شي د احتمالي ګواښونو د پېژندنې وړتيا څو چنده زياته کړي.

له بلې خوا، همدا ټکنالوژي د نويو او پيچلو امنيتي خطرونو د رامنځته کېدو سبب هم ګرځي. سايبري بريدونه، د مصنوعي ځيرکتيا له لارې د غلطو معلوماتو خپرول، د شخصي حريم نقض، د ډيجيټل څارنې زياتوالی، او د اتوماتيکو وسلو پراختيا هغه مهمې ننګونې دي چې د دولتونو ملي امنيت له مستقيم خطر سره مخ کوي. همدارنګه، د دې ټکنالوژۍ ناسم يا غير کنټرول شوی استعمال کولای شي د نړيوالو قدرتي توازنونو په جوړښت کې هم بدلون راولي.

د همدې وضعيت له امله، د ملي امنيت مفهوم نور يوازې د پوځي ځواک په چوکاټ کې نه شي محدودېدلای، بلکې اوس بايد په کې سايبري امنيت، معلوماتي امنيت، ټکنالوژيکي حاکميت او د مصنوعي ځيرکتيا مديريت هم شامل شي. دا بدلونونه دا پوښتنه لا مهمه کوي چې دولتونه څنګه کولای شي د نويو ټکنالوژيو له پرمختګ څخه ګټه واخلي، پرته له دې چې خپل امنيت له خطر سره مخ کړي.

له همدې امله، د دې څېړنې اساسي مسله دا ده چې:

مصنوعي ځيرکتيا او نورې نوې ټکنالوژۍ د دولتونو پر ملي امنيت څه ډول څو اړخيز اغېز لري، او دا اغېزې تر کومه حده د ملي امنيت د پياوړتيا يا کمزورۍ سبب ګرځي.

دا څېړنه هڅه کوي چې د همدې پوښتنې په رڼا کې د مصنوعي ځیرکتیا د مثبتو او منفي اغېزو ترمنځ توازن وځېړي او د معاصر نړیوال امنیت په بدلېدونکي ماهیت کې د دې ټکنالوژۍ رول په علمي ډول تحلیل کړي.

د څېړنې پوښتنې

اصلي پوښتنه:

نوې ټکنالوژۍ، په ځانګړي ډول مصنوعي ځیرکتیا، د دولتونو پر ملي امنیت څه ډول او څو اړخیز اغېز لري؟

فرعي پوښتنې:

۱. مصنوعي ځیرکتیا د ملي امنیت په بېلابېلو برخو کې کوم فرصتونه او ګواښونه ،ننګونې رامنځته کوي؟

۲. دولتونه څنګه کولی شي له نویو ټکنالوژیو څخه د ملي امنیت د پیاوړتیا لپاره اغېزمنه ګټه پورته کړي؟

د څېړنې فرضیې

اصلي فرضیه:

۱. داسې انګېرل کېږي چې نوې ټکنالوژۍ، په ځانګړي ډول مصنوعي ځیرکتیا، د دولتونو پر ملي امنیت څو اړخیز اغېز لري، چې په کې هم فرصتونه او هم ګواښونه شامل دي.

فرعي فرضیې:

۱. داسې انګېرل کېږي چې مصنوعي ځیرکتیا د ملي امنیت په بېلابېلو برخو کې مهم فرصتونه (لکه د معلوماتو چټکه شننه او د پرېکړې نیونه) او همدارنګه ګواښونه (لکه سایبري بریدونه او معلوماتي جګړې) رامنځته کوي.

۲. داسې انګېرل کېږي چې دولتونه کولی شي د مناسبو پالیسیو، تخنیکي ظرفیتونو او کنټرولي میکانیزمونو له لارې له نویو ټکنالوژیو څخه د ملي امنیت د پیاوړتیا لپاره اغېزمنه ګټه پورته کړي.

د څېړنې مخینه

په نړیواله کچه د نویو ټکنالوژیو او ملي امنیت ترمنځ اړیکه د معاصرې امنیتي او سیاسي څېړنې له مهمو او پراخو موضوعاتو څخه ګڼل کېږي. د شلمې پېړۍ له وروستیو او د یوویشتمې پېړۍ له پیل سره د معلوماتي انقلاب او ډیجیټل ټکنالوژۍ چټک پرمختګ د نړیوال امنیت په جوړښت کې بنسټیز بدلونونه رامنځته کړي دي. په دې بهیر کې ګڼو علمي څېړنو او کتابونو د مصنوعي ځیرکتیا رول د دولتونو په امنیتي سیاستونو، پوځي ستراتیژیو او سایبري وړتیاوو کې څېړلی او تحلیل کړی دی، خو لا هم اړتیا شته چې دا موضوع په یوه هراړخیز او جامع علمي چوکاټ کې وڅېړل شي.

روشندل (۱۳۹۳هـ ش) په خپل کتاب (د ملي امنیت او نړیوال نظام) کې د ملي امنیت مفهوم د نړیوال نظام په چوکاټ کې تحلیل کړی او څرګندوي چې امنیت یوازې پوځي اړخ نه لري، بلکې سیاسي، اقتصادي او ستراتیژیک ابعاد هم رانغاړي. نجیب محمود (۱۴۰۴هـ ش) په خپل اثر (نړیوال امنیت) کې د نړیوال امنیت بدلېدونکی ماهیت څېړي او ټینګار کوي چې معاصر امنیتي جوړښتونه د نویو ګواښونو له امله په دوامداره بدلون کې دي. همدارنګه سیف‌زاده (۱۳۸۵هـ ش) په خپل کتاب (د امنیت معما او د

لوړديځې نړۍ نوې ننګونې) کې د معاصر امنیت پېچلتیا او نوې ننګونې تحلیل کړې دي.روزنا او همکاران (۱۳۹۰هـ ش) په خپل اثر (د معلوماتو انقلاب، امنیت او نوې ټکنالوژۍ) کې څرګندوي چې معلوماتي انقلاب د نړیوال امنیت ماهیت بدل کړی او د دولتونو ترمنځ د ځواک توازن یې اغېزمن کړی دی، ځکه چې ټکنالوژي اوس د قدرت یو مهم عنصر ګڼل کېږي.

له بلې خوا، مبین (۱۴۰۲هـ ش) په خپل کتاب (مصنوعي ځیرکتیا) کې د مصنوعي ځیرکتیا بنسټیز مفاهیم او عملي کارونې تشریح کړي دي. احمدي او همکاران (۲۰۲۲م) په خپله مقاله (په ملي امنیت او د هېوادونو په ځواک کې د نویو ټکنالوژیو رول: فرصتونه او ګواښونه) کې څرګندوي چې نوې ټکنالوژۍ هم د دولتونو لپاره فرصتونه رامنځته کوي او هم جدي ګواښونه.

الن او چان (۲۰۱۷م) په خپل راپور (مصنوعي ځیرکتیا او ملي امنیت) کې ټینګار کوي چې مصنوعي ځیرکتیا کولای شي د پوځي برترۍ، معلوماتي تحلیل او اقتصادي ځواک په برخو کې د دولتونو ترمنځ توازن بدل کړي. د کانګرس د څېړنې خدمت (۲۰۱۸م) په خپل راپور (مصنوعي ځیرکتیا او ملي امنیت) کې د مصنوعي ځیرکتیا امنیتي خطرونه، په ځانګړې ډول سایبري جګړې او اتوماتیک وسلو ته اشاره کوي. بوکانن (۲۰۲۰م) په خپل تحلیل (د مصنوعي ځیرکتیا درې ګونی جوړښت او د ملي امنیت ستراتیژي) کې څرګندوي چې مصنوعي ځیرکتیا د ملي امنیت دوديز مفهوم له سره تعریفوي.په سیمه‌ییزه کچه، ساروار او رشید (۲۰۲۵م) په خپله مقاله (د پاکستان په ملي امنیتي ستراتیژۍ کې د مصنوعي ځیرکتیا پرمختګ او اغېزې) کې د مصنوعي ځیرکتیا رول د دولتونو په امنیتي ستراتیژیو کې څېړلی دی. خان (۲۰۲۴م) په خپل اثر (په ملي امنیت کې مصنوعي ځیرکتیا: فرصتونه او ګواښونه) کې د مصنوعي ځیرکتیا دوه ګونی ماهیت تحلیل کړی دی. سپاهر (۲۰۲۴م) په خپل څېړنیز راپور (رېوین سېنټري: په افغانستان کې د مصنوعي ځیرکتیا کارول د خبرداري او څارنې لپاره) کې د مصنوعي ځیرکتیا عملي استعمال د امنیتي څارنې په برخه کې تشریح کړی دی.که څه هم پورته څېړنو د مصنوعي ځیرکتیا او ملي امنیت ترمنځ اړیکه په ښه‌ډول رڼا اچولې ده، خو ډېری یې یا یوازې په پوځي او استخباراتي برخو تمرکز لري او یا یوازې سایبري امنیت ته محدودې دي. لا هم اړتیا شته چې دا موضوع په یوه جامع علمي چوکاټ کې وڅېړل شي څو د مصنوعي ځیرکتیا ټول سیاسي، اقتصادي، پوځي، سایبري او ټولنیز ابعاد په ګډه تحلیل شي.

له همدې امله، دا څېړنه هڅه کوي چې دا علمي تشه ډکه کړي او د مصنوعي ځیرکتیا او ملي امنیت ترمنځ اړیکه په هراړخیز، تحلیلي او منظم ډول وڅېړي.

د څېړنې ارزښت او اړتیا

د دې څېړنې ارزښت په دې کې نغښتی دی چې په معاصر نړیوال نظام کې نوې ټکنالوژۍ، په ځانګړې ډول مصنوعي ځیرکتیا، د دولتونو د ځواک، ثبات او ملي امنیت له اساسي ټاکونکو عناصرو څخه ګرځېدلې دي. په اوسني وخت کې د امنیت مفهوم یوازې له دودیزو پوځي ګواښونو سره محدود نه دی پاتې، بلکې معلوماتي، سایبري، ټکنالوژیکي او استخباراتي ابعاد یې هم تر پوښښ لاندې راغلي دي، چې مصنوعي ځیرکتیا پکې محوري رول لوبوي.

په همدې اساس، د مصنوعي ځیرکتیا د فرصتونو او ګواښونو علمي پېژندنه او تحلیل د دې امکان برابروي چې د دولتونو د پالیسۍ جوړوونکي د ملي امنیت لپاره داسې ستراتیژۍ او تګلارې جوړې کړي چې هم د نویو ټکنالوژیو له مثبتو اغېزو څخه اعظمي ګټه واخلي او هم د احتمالي خطرونو مخنیوی وکړي. دا موضوع په ځانګړې ډول د سایبري امنیت، دفاعي سیستمونو، استخباراتي تحلیلونو او د تصمیم نیونې په بهیر کې ځانګړی اهمیت لري.

له بلې خوا، د دې څېړنې اړتیا له دې ځایه هم راولاړېږي چې په نړیواله کچه د مصنوعي ځیرکتیا د چټک پرمختګ له امله د قدرت توازن، امنیتي سیاستونه او د دولتونو ترمنځ سیالۍ په ژور بدلون کې دي. له همدې امله، د دې ټکنالوژۍ د اغېزو علمي او انتقادي تحلیل د دې لپاره اړین دی چې دولتونه وکولای شي د بدلېدونکي امنیتي چاپېریال سره ځان عیار کړي.

سربېره پر دې، دا څېړنه د ملي امنیت او ټکنالوژۍ په برخه کې د علمي ادبیاتو د بډاینې او پراختیا سبب ګرځي، ځکه چې موجوده څېړنې تر ډېره د موضوع یوازې ځینې اړخونه څېړي، حال دا چې یو هراړخیز او منظم تحلیل لا هم د علمي اړتیا په توګه پاتې دی.

په پایله کې ویل کېدای شي چې دا څېړنه نه یوازې علمي ارزښت لري، بلکې عملي اهمیت هم لري، ځکه چې کولی شي د معاصر امنیتي سیاست په جوړښت کې د تصمیم نیونکو لپاره مهم بنسټیز معلومات او تحلیلي چوکاټ وړاندې کړي.

د څېړنې موخې

۱. د نویو ټکنالوژیو، په ځانګړې ډول مصنوعي ځیرکتیا، پر ملي امنیت د اغېزو هراړخیزه څېړنه او تحلیل ترسره کول.

۲. د مصنوعي ځیرکتیا له مخې د رامنځته کېدونکو فرصتونو او ګواښونو پېژندنه او علمي ارزونه.

۳. د ملي امنیت د پیاوړتیا لپاره د عملي، علمي او اغېزمنو لارو چارو او ستراتیژیو وړاندې کول، په ځانګړې ډول د نویو ټکنالوژیو په رڼا کې.

د څېړنې میتودولوژي

دا څېړنه د علمي میتود له مخې د توصیفي–تحلیلي کړنلارې پر بنسټ ترسره شوې ده. په دې طریقي کې د نویو ټکنالوژیو، په ځانګړې ډول مصنوعي ځیرکتیا، او ملي امنیت ترمنځ اړیکه په لومړي پړاو کې په تفصیلي او تشریحي ډول بیان شوې او وروسته په تحلیلي بڼه ارزول شوې ده، څو د موضوع بېلابېل اړخونه په روښانه، منظم او علمي ډول څرګند شي.

د معلوماتو د راټولولو لپاره له کتابتوني سرچینو څخه ګټه اخیستل شوې ده. په دې سرچینو کې علمي کتابونه، څېړنیزې مقالې، نړیوال او سیمه‌ییز راپورونه، علمي مجلې او معتبر اکادمیک انټرنېټي اسناد شامل دي. دغه مواد په منظم ډول راټول، څېړل شوي او د موضوع د اړتیاوو له مخې طبقه‌بندي شوي دي، څو د تحلیل لپاره منظم بنسټ برابر شي.

د معلوماتو تحلیل په کیفي بڼه ترسره شوی دی، یعنې تمرکز د شمېرنو پر ځای د مفاهیمو، نظریو، علمي استدلالونو او د لیکوالانو د نظریاتو پر ژور شننه شوی دی. په دې بهیر کې د بېلابېلو علمي سرچینو

نظريات سره پرتله شوي، د هغوی ترمنځ ورته والی او توپيرونه روښانه شوي، او له دې تحليل څخه علمي پايلې او استنتاجونه ترلاسه شوي دي.

همدارنګه په دې څېړنه کې هڅه شوې چې د مصنوعي ځيرکتيا د اغېزو بېلابېل اړخونه لکه پوځي، استخباراتي، سايبري، اقتصادي او ټولنيز ابعاد په ګډه وڅېړل شي، څو څېړنه يوازې په يوه محدود زاويه کې پاتې نه شي، بلکې هراړخيز او متوازن تحليلي بڼه ولري.

په پای کې دا څېړنه د موجودو علمي منابعو پر بنسټ د مصنوعي ځيرکتيا او ملي امنيت ترمنځ اړيکه په منظم، هراړخيز او ژور علمي چوکاټ کې څېړي، څو د موضوع د ښه درک او علمي تحليل لپاره معتبر بنسټ وړاندې کړي.

لومړی څپرکی: مفهومونه او نظري چوکاټ

په دې څپرکي کې د څېړنې بنسټیز مفاهیم او نظري چوکاټ په منظم او علمي ډول تشریح کېږي، څو لوستونکی د موضوع له اساسي اصطلاحاتو او مفاهیمو سره بلد شي. لومړی د نویو ټکنالوژیو عمومي تعریف وړاندې کېږي، چې د معاصرې نړۍ په ښلاښلو برخو کې یې د انسان پر ژوند، اقتصاد، سیاست او امنیت ژور اغېز کړی دی. ورپسې د مصنوعي ځیرکتیا مفهوم ته ځانګړې پاملرنه کېږي، چې د نویو ټکنالوژیو له مهمو او پرمختللو بڼو څخه ګڼل کېږي او ماشینونو ته د معلوماتو د درک، تحلیل او پرېکړې نیونې وړتیا ورکوي. وروسته د امنیت مفهوم تشریح کېږي او د هغه اهمیت د فردي او ټولنیز ژوند په کچه روښانه کېږي، ځکه امنیت د انساني ژوند له اساسي اړتیاوو څخه شمېرل کېږي. همدارنګه، د ملي امنیت مفهوم، چې د دولتونو د بقا، ثبات او پرمختګ له مهمو عناصرو څخه دی، په تفصیل سره بیانېږي. په پای کې، هڅه کېږي چې د دغو مفاهیمو ترمنځ اړیکې روښانه شي، څو د مصنوعي ځیرکتیا او ملي امنیت ترمنځ د اړیکې د لا ښه درک لپاره یو روښانه نظري بنسټ برابر شي.

لومړی مبحث: د نویو ټکنالوژیو مفهوم او پېژندنه

ټکنالوژي د انساني پوهې، مهارتونو، وسایلو، طریقو او علمي لاسته راوړنو هغې ټولګې ته ویل کېږي چې انسان ترې د خپلو ستونزو د حل، د خدمتونو او د توکو د تولید، او د ژوند د کیفیت د ښه والي لپاره ګټه ترې اخلي. د بشري تمدن له پیل څخه تر نن ورځې پورې ټکنالوژي د انسان د پرمختګ له بنسټیزو عواملو څخه ګڼل کېږي.

د علم او تخنیک د چټک پرمختګ، د ټولنو د نویو اړتیاوو او د نړیوالې سیالۍ له زیاتېدو سره، د ټکنالوژۍ یوه نوې بڼه رامنځته شوې ده چې د نوې ټکنالوژۍ په نوم یادیږي. نوې ټکنالوژۍ هغه پرمختللې ټکنالوژۍ دي چې د معاصرو علومو، نوښت، څېړنې او پرمختیا پر بنسټ رامنځته شوې وي او د دودیزو ټکنالوژیو په پرتله لوړ دقت، چټکتیا، موثریت او هوښیارتیا لري. په عمومي ډول، د نوې ټکنالوژۍ مفهوم یو متحرک او بدلېدونکی مفهوم دی، ځکه چې هغه څه چې نن نوې ټکنالوژي بلل کېږي، ښایي په راتلونکو کلونو کې عادي او دودیزه وګڼل شي.

لومړی بیان: د نویو ټکنالوژیو تعریف

د «نوې ټکنالوژۍ» اصطلاح د هغو نوو او نوښتګرو لارو چارو کارونې ته ویل کېږي، چې د وسایلو، کړنلارو او سیستمونو د طرحې، پراختیا او عملي کېدو په بهیر کې کارول کېږي، او پایله یې د ګټې اخیستنې لوړېدل، د لګښتونو کمېدل، د خدمتونو د کیفیت ښه کېدل او د نوو کاري فرصتونو رامنځته کېدل وي.

دا ډول ټکنالوژۍ زیاتره پر لوړې پوهې او نوښت ولاړې وي، او کولای شي د اقتصاد او انساني ژوند په ټولو برخو کې ژور اغېز ولري.[1] نوې ټکنالوژۍ معمولاً داسې برخې رانغاړي لکه مصنوعي ځیرکتیا، د

[1] مصنوعي ځیرکتیا (Artificial Intelligence - AI) هغه ټکنالوژي ده چې ماشینونو ته د انسان په څېر د فکر او زده‌کړې وړتیا ورکوي، د شیانو انټرنېټ (Internet of Things - IoT) بیا فزیکي وسایل د انټرنېټ له لارې سره نښلوي او معلومات تبادله کوي. بلاک‌ځنځیر (Blockchain) یو خوندي ډیجیټلي سیستم دی چې معلومات په غیرمتمرکز ډول ثبتوي او د درغلۍ مخه نیسي. د بیا نوي کېدونکو انرژیو کارونه (Renewable Energy) هغه سرچینې رانغاړي چې تل بیا تولیدېږي لکه لمر او باد. نانو ټکنالوژي (Nanotechnology) د ډېرو کوچنیو ذرو په کچه کار کوي، او بیوټکنالوژي (Biotechnology) د ژوندیو موجوداتو له لارې په طب، کرنه او صنعت کې ګټه ورنه اخیستل کیږي.

شیانو انټرنېټ، بلاک ځنځیر، د بیا نوي کېدونکو انرژیو کارونه، نانو ټکنالوژي، بایولوژي او ډېرې نورې (تاپ ناپ، ۲۰۲۵/۱۴۰۴).

او یا په بل عبارت،نوې ټکنالوژۍ هغو پرمختللو علمي او تخنیکي وسایلو ته ویل کېږي چې د انساني ژوند په بېلابېلو برخو کې د اسانتیا، چټکتیا او موثریت سبب ګرځي. دغه ټکنالوژۍ د معلوماتو راټولولو، تحلیل، لېږد او مدیریت په برخه کې مهم رول لري او د دولتونو په سیاسي، اقتصادي، پوځي او امنیتي جوړښتونو کې بنسټیز بدلونونه رامنځته کوي. مصنوعي ځیرکتیا، سایبري سیستمونه او ډیجټلي شبکې د نویو ټکنالوژیو مهمې بېلګې دي چې د ملي امنیت په تامینولو کې اغېزناک رول لوبوي. او همدارنګه نوې ټکنالوژۍ یو لړ بنسټیزې ځانګړتیاوې لري چې له امله یې له دودیزو ټکنالوژیو څخه جلا کېږي. دا ځانګړتیاوې د نوې ټکنالوژۍ علمي بڼه څرګندوي او د ټولنې په اقتصادي، علمي او ټولنیزو بدلونونو کې یې ارزښت روښانه کوي. د نوې ټکنالوژۍ مهمې ځانګړتیاوې په لاندې ډول دي:

۱. د پوهې پر بنسټ ولاړه ټکنالوژۍ

د نوې ټکنالوژۍ تر ټولو مهمه ځانګړتیا د پوهې پر بنسټ ولاړېدل دی. دا ټکنالوژۍ د معاصرو علومو، علمي څېړنو، تجربوي مطالعاتو او د څېړنې او پراختیا پر بنسټ رامنځته کېږي. د دودیزو ټکنالوژیو برعکس، چې زیاتره پر عملي تجربو او لاسي مهارتونو ولاړې وې، نوې ټکنالوژۍ د لوړې علمي پوهې، تخنیکي مهارتونو او تخصص غوښتنه کوي.

د پوهې پر بنسټ ولاړتیا د دې لامل ګرځي چې نوې ټکنالوژۍ د دوامدار پرمختګ وړتیا ولري او د اقتصاد د د پوهې پر بنسټ ولاړ کېدو زمینه برابره کړي.[۱]

۲. نوښتونه او خلاقیتونه

نوښت او خلاقیت د نوې ټکنالوژۍ له بنسټیزو ځانګړتیاوو څخه شمېرل کېږي. دا ټکنالوژۍ تل د بدلون، پرمختګ او اصلاح په حال کې وي او د ثابت حالت څخه تېرېږي. نوښت په نوې ټکنالوژۍ کې د نویو نظریو، محصولاتو او خدماتو رامنځته کول دي، یا د موجوده سیستمونو بنسټیز بڼه والی دی.

خلاقیت د دې سبب ګرځي چې د انساني ستونزو لپاره نوې او اغېزمنې حل لارې وړاندې شي او د ټولنې بدلېدونکو اړتیاوو ته مناسب ځواب ورکړل شي.[۲]

۳. لوړه چټکتیا او موثریت

نوې ټکنالوژۍ د لوړې چټکتیا او موثریت لرونکې دي. د دې ټکنالوژیو په مرسته پېچلي او وخت‌نیوونکي کارونه په ډېر کم وخت او لوړ دقت سره ترسره کېږي.

د بېلګې په توګه، د معلوماتو د پروسس او تحلیل بهیرونه چې پخوا ډېر وخت نیوه، اوس د نوې ټکنالوژۍ له لارې په څو شېبو کې ممکن شوي دي. دا چټکتیا د وخت، لګښت او انساني سرچینو د سپما سبب ګرځي.[۳]

---

[۱] Knowledge-Based

[۲] Innovation and Creativity

[۳] High Speed and Efficiency,Data Processing,Data Analysis

۴. هوښیارتیا او خودکار توب

هوښیارتیا او ځیرکتیا د نوې ټکنالوژۍ له مهمو ځانګړتیاوو څخه ده. زیاتره نوې ټکنالوژۍ د مصنوعي ځیرکتیا، ماشیني زده‌کړې او هوښیارو سیستمونو څخه ګټه پورته کوي.

خودکار توب یا دا چې یو کار په خپل سر ترسره شي، دا امکان برابروي چې ډېر تکراري او ستړي کوونکي کارونه د ماشینونو له‌خوا ترسره شي، چې دا چاره د انساني تېروتنو کچه راکموي او د کار کیفیت لوړوي.[۱]

۵. انعطاف‌پذیري او د تطابق وړتیا

نوې ټکنالوژۍ د انعطاف‌پذیرۍ او د تطابق وړتیا لوړه کچه لري. دا ټکنالوژۍ کولای شي د وخت له بدلونونو، د بازار له غوښتنو او د کارووونکو له اړتیاوو سره ځان عیار کړي. دغه ځانګړتیا د دې لامل ګرځي چې نوې ټکنالوژۍ په بېلابېلو برخو کې په بریالۍ توګه وکارول شي.[۲]

٦. پراخ او څو اړخیز اغېز

نوې ټکنالوژۍ پراخ او څو اړخیز اغېز لري او یوازې په یوه برخه پورې محدودې نه دي. دا ټکنالوژۍ په اقتصاد، زده‌کړه، روغتیا، کلتور او ټولنیزو اړیکو ژور اغېز کوي.

د بېلګې په توګه، ډیجیټلي ټکنالوژۍ نه یوازې اقتصادي جوړښتونه بدل کړي، بلکې د خلکو د ژوند ډول او د اړیکو طریقې یې هم بدلې کړې دي(ویکي‌پدیا، ۱۴۰۴).

دوهم بیان : د نویو ټکنالوژیو ډولونه

نوې ټکنالوژۍ بېلابېل ډولونه لري چې هر یو یې په معاصره نړۍ کې مهم رول لري. دا ټکنالوژۍ نه یوازې اقتصادي او صنعتي پرمختګ ته لاره هواروي، بلکې د امنیت، سیاست، روغتیا او ټولنیزو اړیکو په بدلون کې هم بنسټیز اغېز لري. تر ټولو مهم ډولونه یې په لاندې ډول دي:

۱. مصنوعي ځیرکتیا: مصنوعي ځیرکتیا هغه پرمختللې ټکنالوژي ده چې ماشینونو ته د انسان په څېر د فکر کولو، تحلیل کولو، زده‌کړې او پرېکړې کولو وړتیا ورکوي. دغه سیستمونه کولای شي له معلوماتو څخه زده کړه وکړي او د وخت په تېرېدو سره خپله کړنه لا ښه کړي. دا ټکنالوژي په پوځي چارو، استخباراتي تحلیل، سایبري امنیت، روغتیایي تشخیص او اقتصادي وړاندوینو کې کارېږي او د ګواښونو په پېژندنه کې مهم رول لري.

۲. د شیانو انټرنېټ: د شیانو انټرنېټ هغه شبکه ده چې پکې فزیکي وسایل لکه سنسرونه، کمرې او نور ډیجیټلي وسایل د انټرنېټ له لارې یو له بل سره نښلول کېږي. دغه وسایل کولای شي معلومات راټول او یو له بل سره یې شریک کړي. د دې ټکنالوژۍ کارونه په سمارټ ښارونو، کرنه، صنعت او امنیتي څارنه کې ډېر پراخ دي.

[۱] Intelligence, Automation, Artificial Intelligence (AI), Machine Learning, Smart Systems.
[۲] Flexibility, Adaptability, Education, Health, Industry, Management

۳. بلاک ځنځیر ټکنالوژي: بلاک ځنځیر یو غیرمتمرکز ډیجیټلي سیستم دی چې معلومات په خوندي ډول ثبتوي او بدلون پکې ډېر ستونزمن وي. دا ټکنالوژي په مالي چارو، ډیجیټلي قراردادونو او د معلوماتو په خوندیتوب کې کارېږي او د شفافیت او باور د زیاتوالي سبب ګرځي.
۴. د بیا نوي کېدونکې انرژۍ ټکنالوژۍ:دا ټکنالوژۍ د طبیعي سرچینو لکه لمر، باد او اوبو څخه انرژي تولیدوي. دا انرژي دوامداره ده او چاپېریال ته لږ زیان رسوي. د انرژۍ د خوندیتوب او چاپېریال ساتنې لپاره یې ارزښت ډېر لوړ دی.
۵. نانو ټکنالوژي: نانو ټکنالوژي د موادو په ډېره کوچنۍ کچه کار کوي او د نوو ځانګړتیاوو لرونکي مواد جوړوي. دا ټکنالوژي په طب، صنعت او دفاعي چارو کې کارېږي او د راتلونکي له مهمو علمي برخو څخه شمېرل کېږي.
٦. بیولوژیکي ټکنالوژي: بیولوژیکي ټکنالوژي د ژوندیو موجوداتو او بیولوژیکي سیستمونو څخه د انساني ګټې لپاره کار اخلي. دا ټکنالوژي په درمل جوړونه، کرنه او روغتیا کې مهم رول لري او د انسان د ژوند د ښه والي لامل ګرځي.
۷. لوي معلومات (لویه ډاټا): لوي معلومات د ډېرو او پېچلو معلوماتو راټولولو او تحلیل ته ویل کېږي. دا معلومات د پرېکړو په کولو، د ګواښونو په پېژندنه او د راتلونکو حالاتو په اټکل کې مرسته کوي او په حکومتي او اقتصادي برخو کې ډېر ارزښت لري.[1]

درېیم بیان : مصنوعي ځیرکتیا

د مصنوعي ځیرکتیا تاریخي مخینه، په ۱۹۵۰ کال کې آلن تورینګ د «تورینګ ازموینه» وړاندیز وکړ، تر څو وڅېړل شي چې آیا ماشین کولای شي د انسان په څېر فکر وکړي او که نه. ۱۹۵۱ کال د لوبو په برخه کې د مصنوعي ځیرکتیا د عملي کارونې کال بلل کېږي؛ په همدې کال کې کریستوفر سټراچي د «چکرز» لوبې لپاره یو پروګرام جوړ کړ او ډیټریش پرینز د شطرنج لپاره یو بل پروګرام ولیکه.
۱۹۵٦ کال د مصنوعي ځیرکتیا په تاریخ کې تر ټولو مهم کال ګڼل کېږي؛ ځکه چې جان مک‌کارتي په همدې کال کې د دارتموث په کنفرانس کې د لومړي ځل لپاره د «مصنوعي ځیرکتیا» اصطلاح وکاروله. وروسته، په ۱۹۵۹ کال کې د مصنوعي ځیرکتیا لومړنی لابراتوار، یعنې د ماساچوسټس ټکنالوژۍ انسټیټیوټ د مصنوعي ځیرکتیا لابراتوار جوړ شو او په دې برخه کې څېړنې پیل شوې.
په ۱۹٦۱ کال کې د مصنوعي ځیرکتیا لومړنی چټ‌بات، چې یو هوښیار مجازي مرستیال و او «الیزا» نومېده، معرفي شو(میتال، ۲۰۲۰: ۲۵). د ۱۹۸۰مې لسیزې په جریان کې، مصنوعي ځیرکتیا د دوو مهمو عواملو له امله بېرته وده وموندله: د الګوریتمي وسایلو پراختیا او د پانګونې زیاتوالی. جان هاپفیلډ او ډېوډ رومل‌هارت د ژورې زده‌کړې تخنیکونه دود کړل، چې له مخې یې کمپیوټرونه کولای شول د تجربې پر بنسټ زده‌کړه وکړي. له بلې خوا، اډوارډ فایګنباوم د «کارپوه سیستمونو» مفکوره وړاندې کړه، چې د انسان د متخصص د پرېکړه‌نیولو بهیر تقلیدوي(انیوها، ۲۰۱۷). یادونه ؛ د تورینګ ازموینه، چې په ۱۹۵۰

[1] Artificial Intelligence, Internet of Things, Blockchain, Renewable Energy Technologies, Nanotechnology, Biotechnology, Big Data

کال کې د آلن تورینګ له خوا وړاندیز شوه، د ماشین د دې وړتیا د ارزونې لپاره کارپږي چې داسې هوښیار چلند وښیي چې د انسان له چلند څخه ښلېدونکی نه وي. په دې ازموینه کې یو انساني ارزونکی د متن له لارې هم له انسان او هم له ماشین سره اړیکه نیسي؛ که ارزونکی ونه‌کولای شي په باور وړ ډول د دواړو ترمنځ توپیر وکړي، نو ویل کېږي چې ماشین دغه ازموینه بریالی ټېره کړې ده(رای، ۲۰۲۴: ۳).

څلورم بیان: د مصنوعي ځیرکتیا تعریف او پیژندنه

مصنوعي ځیرکتیا د معاصرې ټکنالوژۍ له مهمو او پرمختللو مفاهیمو څخه ده چې د کمپیوټري علومو په چوکاټ کې د هوښیارو سیستمونو د جوړولو او پراختیا سره تړاو لري. د دې مفهوم د ښه درک لپاره، ښلاښلو پوهانو او څېړونکو ښلاښل تعریفونه وړاندې کړي دي.د مصنوعي ځیرکتیا له بنسټ اېښودونکو څخه جان مک‌کارتي مصنوعي ځیرکتیا داسې تعریف کړې ده چې دا د هغو هوښیارو ماشینونو د جوړولو علم او انجنیري ده چې د انسان په څېر فکر کولای شي او ستونزې حل کړي (مک‌کارتي، ۱۹۵٦).

همدارنګه، ستوارټ رسل او پیټر ناروېګ مصنوعي ځیرکتیا د هغو هوښیارو عاملانو د مطالعې په توګه تعریفوي چې خپل چاپېریال درک کوي او داسې کړنې ترسره کوي چې د خپلو موخو د ترلاسه کولو احتمال زیات کړي (رسل او ناروېګ، ۲۰۲۱). له بلې خوا، ایلین ریچ مصنوعي ځیرکتیا د کمپیوټري علومو هغه څانګه ګڼي چې هڅه کوي داسې کارونه ترسره کړي چې که انسان یې ترسره کړي، نو هوښیار به وبلل شي (ریچ، ۱۹۸۳).

همدارنګه، نیلس نیلسن مصنوعي ځیرکتیا د داسې ماشینونو د جوړولو فعالیت بولي چې هوښیار چلند وکړي (نیلسن، ۱۹۹۸). په همدې ډول، پاتریک وینسټن مصنوعي ځیرکتیا د هغو مفاهیمو مطالعه ګڼي چې د کمپیوټرونو له لارې د استدلال، زده‌کړې او هوښیار چلند امکان برابروي (وینسټن، ۱۹۹۲).

د پورته تعریفونو پر بنسټ، ویلای شو چې مصنوعي ځیرکتیا د کمپیوټري علومو هغه څانګه ده چې د داسې سیستمونو د جوړولو او پراختیا هڅه کوي چې د انسان په څېر د معلوماتو درک، زده‌کړه، تحلیل، استدلال او پرېکړه‌نیونه ترسره کړي.

جدول ۱: د مصنوعي ځیرکتیا شاخصونه (محمدي منفرد او تقي‌پور جاوي، ۱۴۰۳: ۲۹۱–۲۹۲)

لومړی شاخص: د انسان په څېر تفکر یا فکر کول.[۱]	**دریم شاخص: عقلاني تفکر یا سوچ کول.**[۱]
د کمپیوټر د فکر کولو لپاره نوې او جالبه هڅه؛ یعنې داسې ماشینونه جوړول چې په واقعي معنا ذهني وړتیا ولري (هوګلنډ، ۱۹۸۵). د هغو فعالیتونو اتومات کول چې د انسان له فکر سره تړاو لري؛ لکه د پرېکړې نیول، د ستونزو حل او زده کړه (بېلمن، ۱۹۸۷).	د محاسبوي ماډلونو په مرسته د ذهني وړتیاوو مطالعه (چارنیک او مک‌ډرموټ، ۱۹۸۵). د هغو محاسباتو مطالعه چې ادراک، استدلال او عمل ممکن کوي (وینسټن، ۱۹۹۲).
دویم شاخص: د انسان په څېر عمل کول .[۱]	**څلورم شاخص: عقلاني عمل کول.**[۱]
د داسې ماشینونو جوړولو هنر چې هغه دندې ترسره کړي کومې چې د انسان له خوا د ترسره کېدو پر مهال ځیرکتیا ته اړتیا لري (کرزویل، ۱۹۹۰) ددی مطالعه چې څنګه کولای شو کمپیوټرونو سیستم داسې کارونه ترسره کړي چې اوس مهال انسانان یې تر هغوی ښه ترسره کوي (نایټ او ریچ، ۱۹۹۱).	محاسبوي ځیرکتیا د هوښیارو عاملانو (هوښیار اجنټان) د طراحي مطالعه ده (پول او نور، ۱۹۹۸). مصنوعي ځیرکتیا د مصنوعي جوړښتونو د هوښیار چلند سره تړاو لري. (نیلسن، ۱۹۹۸)

پنځم بیان : د مصنوعي ځیرکتیا بنسټیز عنصرونه

د مصنوعي ځیرکتیا د درک او پیژندنې وړتیا څو مهم عنصرونه لري.

الګوریتمونه: مصنوعي ځیرکتیا پر الګوریتمونو متکي ده. د مصنوعي ځیرکتیا ببلابېلو اړخونو لکه د نمونې تشخیص ، تصمیم نیونې او یاد ساتنې ته د رسېدلو لپاره دا الګوریتمونه له ډېټا څخه جوړېږي. الګوریتمونه د هغو لارښوونو ټولګه او یا هم اجرایي سلسله مراتب او ګام په ګام میتودونه دي چې د یوې ځانګړې ستونزې د حل او یا هم د یو خاص کار د کولو لپاره طرح شوي دي او د کمپیوټري سیستمونو په وسیله د اطلاعاتو پر پروسس کولو عمل کوي، چې ببلګې تشخیص کړي، وړاندوینې وکړای شي او پروسس په ښه شکل ترسره کړي.[۱]

ډېټا : هغه معلومات او یا اطلاعات دي چې د کمپیوټري سیستمونو په وسیله را ټولېږي، زېرمه او پروسس کېږي. ببلابېل ډولونه لري لکه متن، شمېرې، انځورونه، غږ، ویډیو او یا بل هر ډول ډیجیټالي شي. ډېټا د مصنوعي ځیرکتیا ماشیني زده کړې لپاره بنسټیز حیثیت لري ځکه د همدې په وسیله د مصنوعي ځیرکتیا سیستمونه د یو څه د زده کولو، تصمیم نیولو او یا د یو څه د تولیدولو وړتیا پیدا کوي. د مصنوعي ځیرکتیا په برخه کې عموماً له ډېټا د زده کړیزو ماډلونو لپاره کار اخیستل کېږي.

[۱] pattern recognition

زده کړه او ماشيني زده کړه: د مصنوعي ځيرکتيا ماډلونو ته د معلوماتو په کارولو سره زده کړه ورکول کېږي، تر څو بېلابېل ډولونه، اړيکې او ځانګړتياوې درک کړي او وکولای شي ټاکلې دندې په سمه توګه ترسره کړي. په دې بهير کې د ماډل دننه شمېرنيز ارزښتونه په تدريجي ډول سمول کېږي، څو د ورکړل شويو معلوماتو له مخې د هغه کړنې لا ښې او دقيقې شي. د زده کړې ځينې مهم ډولونه دا دي: تر لارښوونې لاندې زده کړه، بې‌لارښوونې زده کړه، او پياوړتيايي زده کړه. دا ټولې لارې د دې لپاره کارول کېږي چې ماډلونه لا ښه وروزل شي او عملي پايلې يې اغېزمنې او د باور وړ شي.

شننه او پرېکړه نيونه : تر زده کړې وروسته، د مصنوعي ځيرکتيا ماډلونه کولای شي د نويو معلوماتو پر بنسټ پايله تړې واخلي او پرېکړه وکړي. دوی هغه پوهه چې د زده کړې په بهير کې يې تر لاسه کړې وي، د معلوماتو د څېړنې، شننې، نويو داخلېدونکو معلوماتو د ارزونې، پايلو د توليد او يا د وړاندوينې لپاره کاروي.

دا بهير د مصنوعي ځيرکتيا سيستمونو ته دا توان ورکوي چې په انځورونو کې شيان وپېژني، ژبې وژباړي، د محصولاتو سپارښتنه وکړي، ناروغۍ تشخيص کړي او ډېر نور مهم کارونه ترسره کړي.

د پورته عناصرو په مرسته يو کمپيوتري سيستم يا روبوټ کولی شي په اغېزمن او هوښيار ډول خپلې دندې ترسره کړي.

دويم مبحث: د ملي امنيت مفهوم او ابعاد

د امنيت لټون د انسان له تر ټولو مهمو کوښښونو او انګېزو څخه دی. دا کوښښ د انسان د هستۍ له جوهر سره نه بېلېدونکی تړاو لري. د ځان ساتنه او د نفس صيانت د انسان له بنسټيزو غوښتونو څخه ګڼل کېږي. انسانان د خپلو حياتي اړتياوو د پوره کولو په موخه له يو بل سره بېلابېلو اړيکو ته داخليږي او ټولنه جوړوي.

د هرې ټولنې ـ که هغه يوه ټبره يا قبيله وي، او که يو قوم يا هېواد ـ تر ټولو مهمه اړتيا د هماغې ټولنې او د هغې د غړو د امنيت تأمين دی. زمونږ په اوسني عصر کې، واړه ټولنې د «هېواد» په نوم يوه لويه ټولنه جوړوي، او همدغه هېوادونه د نړۍ په کچه د تر ټولو مهمو سياسي واحدونو په توګه راڅرګند شوي دي. د دغو واحدونو د ټوليز قدرت د جوړښت او ماهيت له تکامل سره، نړيوال نظام رامنځته کېږي. په هغه نظام کې چې د وېستفاليا له کانګرې څخه راولاړ شو، تر ټولو لوړه واکمني د هېوادونو پورې اړه لري؛ يعنې هېڅ نړيوال بنسټ يا سازمان ـ نه په عملي (دفکتو) او نه هم په حقوقي (دوژور) بڼه ـ تر هېوادونو لوړ قدرت نه لري، څو هغوی د يوه واحد ټوليز جوړښت يا د يوې نړيوالې ټولنې په توګه اداره کړي.

البته د شلمې پېړۍ له پيل راهيسې، دغه نظام له ځينو بياکتنې (تعديلاتو) سره مخ شوی، او دا تعديلات اوس لا په چټکۍ سره روان دي. له همدې امله، نړيوالې اړيکې په بنسټيز ډول د هېوادونو ترمنځ د اړيکو ټولګه بلل کېږي.

هېوادونه له بېلابېلو اړخونو، لکه مادي او معنوي امکاناتو ـ د بېلګې په توګه: جيوستراتېژيک موقعيت، طبيعي سرچينې، نفوس، د اقتصادي ودې کچه، کورنی انسجام او سياسي ثبات ـ يو له بل سره برابر نه دي. له همدې امله، د نړيوالې ټولنې په چوکاټ کې د خپلو ګټو د حدودو په اړه د هغوی انګېرنې او تمې

یو شان نه دي، او همدارنګه د دغو ګټو د پرمخ بیولو وسایل او امکانات یې سره توپیر لري. د دولتونو ګټې، د ښاښلو لاملونو له مخې، کله ناکله له یو بل سره توپیر لري، او همدغه توپیر د هغوی ترمنځ د اختلاف او کشمکش د راټوکېدو لامل ګرځي. له همدې امله ویلای شو چې د ملي امنیت د تأمین هڅه، او یا د هغه د ساحې پراخول، د نړیوالو اړیکو په ډګر کې د هېوادونو له تر ټولو مهمو موخو څخه دي. د ملي امنیت د کچې لوړول د دولتونو له بنسټیزو اندېښنو څخه شمېرل کېږي او د هغوی د بهرنۍ پالیسۍ له اساسي ستنو څخه یوه ده. د سیاسي او اقتصادي اړیکو ټینګښت، د نظامي او دفاعي توان پیاوړتیا، د متحدینو لټون، د نظامي تړونونو لاسلیک، او له د ټولیز امنیت له نظام سره ملګرتیا، ټول د همدې موخې د ترلاسه کولو لپاره ترسره کېږي.

په دې توګه، له هغه وخته چې خپلسرې ملوکالطوایفي واکمنۍ او سترې امپراتورۍ د ملي دولتونو یا هېواد ـ دولتونو ځای ونیو، او دا ملي دولتونه د نړیوالو اړیکو د اساسي واحدونو په توګه راڅرګند شول، د «ملي امنیت» اصطلاح د دولتي چارواکو او پوځي مشرانو په ژبه جاري شوه.

البته، لکه څنګه چې مخکې یادونه وشوه، د امنیت مفهوم د انساني ټولنو ـ که هغه واړه وي او که سترې ـ له پیدایښته سره همزاد پاتې شوی دی. د لومړنیو ټولنو واړه قبایل، د لرغونې نړۍ سترې امپراتورۍ، او د یونان ښار ـ دولتونه، هېڅ یو هم د امنیت له مفهومه ناخبره نه وو. خو د «ملي امنیت» مفهوم، یعنې هغه اصطلاح چې له دوو کلیمو: امنیت (نوم) او ملي (صفت) څخه جوړه شوې ده، په طبیعي ډول یو نوی مفهوم دی، چې د معاصرې دورې د ملي دولتونو د راپیدا کېدو سره راڅرګند شوی دی.

د نویو ملي دولتونو د رامنځته کېدو د څرنګوالي بحث د دې اثر له حوصلې بهر دی.

په هر صورت، د ملي دولتونو له راپیدا کېدو سره هم‌مهاله د «ملي ګټو» مفهوم او د هغه تر چتر لاندې د «ملي امنیت» مفهوم هم رواج وموند. د ملي امنیت اصطلاح د اوږدې مودې لپاره د سیاستمدارانو او پوځي مشرانو د تکیه‌کلام په توګه کارېدله، پرته له دې چې څوک د هغې د تعریف یا تشریح هڅه وکړي. آن د ټولنیزو او سیاسي علومو څېړونکو او لیکوالانو، سره له دې چې دا مفهوم یې په خپلو لیکنو کې په صراحت او تلویح کار روه، د هغه لپاره یې کوم روښانه تعریف وړاندې نه کړ.

له همدې امله ویلای شو چې د ملي امنیت د مفهوم تعریف او تحلیل چندان پخوانی سابقه نه لري، او په اصل کې له دویمې نړیوالې جګړې وروسته دا مفهوم د ټولنیزو او سیاسي علومو د څېړونکو له خوا د یوه تحلیلي مفهوم او د مطالعې د یوې مستقلې حوزې په توګه تر پام لاندې ونیول شو.

په دې برخه کې تر ټولو لومړني منظم اقدامات د دویمې نړیوالې جګړې وروسته د متحده ایالاتو د ادارې له خوا ترسره شول. متحده ایالات، چې د نړۍ د مشرتابه په دعوه کې یې د انګلستان ځای نیولی و او د شوروي اتحاد د نفوذ د پراختیا پر وړاندې یې د مقابلې مسؤلیت پر غاړه اخیستی و، اړ و چې خپل اوږدمهاله امنیتي پروګرامونه جوړ کړي. د دغو امنیتي پروګرامونو د جوړښت په بهیر کې ـ حتٰی د جګړې د کلونو په ترڅ کې ـ دا څرګنده شوې وه چې د ملي امنیت اړوند د لومړیتوبونو په ټاکلو کې د سیاستمدارانو ترمنځ ژور اختلافات موجود دي.

تخنیکي پرمختګونو، په ځانګړي ډول د اټومي وسلو راپیدا کېدو، په بشپړه روښانتیا سره دا وښودله چې نور د پوځي مسایلو څېړنه نشي کېدای چې له اقتصادي او سیاسي ملاحظاتو څخه جلا او بې‌اړیکې ترسره شي. همدلته د ملي امنیت مسأله څو پوړیزه شوه او نوې ابعاد یې خپل کړل. تر دې وړاندې، د ملي امنیت مفهوم اساساً د پوځي امنیت له مفهوم سره ګډ شوی او په هغه کې مستحیل شوی و. په ۱۹۴۷ میلادي کال کې د امریکا کانګرېس د «ملي امنیت قانون» تصویب کړ، چې موخه یې د هغو سیاستونو، کړنلارو، سازمانونو او دولتي دندو د پلي کېدو لپاره زمینه برابرول وو، کوم چې د ملي امنیت د تأمین لپاره اړین بلل کېدل. د دې قانون له تصویب وروسته، ګڼ شمېر بنسټونه د ملي امنیت د مسایلو د څېړنې لپاره جوړ شول، او له څېړونکو وغوښتل شول چې په دې برخه کې پراخې مطالعې او څېړنې ترسره کړي. که څه هم تر دې وړاندې هم ځینې پرکنده علمي هڅې شوې وې ـ د بېلګې په توګه د چارلز بېرد، جېمز مېډیسن او هانس مورګنتاو له خوا ـ خو په بنسټیز ډول، یوازې د دولتي څېړنیزو مؤسسو له تأسیس وروسته د ملي امنیت په برخه کې منظم او سیستماتیک مطالعات پیل شول(روشندل، ۱۳۸۸: ۳-۶).

لومړی بیان: د ملي امنیت تعریف

ملي امنیت د دولت هغه حالت ته ویل کېږي چې په کې د هېواد سیاسي خپلواکي، ځمکنۍ بشپړتیا، ملي ګټې او د خلکو امن خوندي وي. ملي امنیت د دولت د بقا او ثبات اساسي رکن ګڼل کېږي او د کورنیو او بهرنیو ګواښونو پر وړاندې د دولت د دفاع توان خرګندوي. د ملي امنیت لپاره بېلابېل تعریفونه وړاندې شوي دي. ځینو لیکوالانو امنیت د پوځیز ګواښ د نشتون په مانا اخیستی دی. ځینې نور بیا پر دې ټینګار کوي چې امنیت د هېواد ساتنه ده، د بهرني پوځیز برید یا له بهر څخه د نظام د نړولو د هڅو پر وړاندې. د دې مفهوم له پېژندل شوو تعریفونو څخه یو هم د هغه دودیز (کلاسیک) تعریف دی. د دې تعریف له مخې، امنیت د هېواد هغه وړتیا ده چې وکولای شي د خپلو سیاسي بنسټونو یا ملي ګټو پر وړاندې بهرني ګواښونه شنډ او دفع کړي.

په دغو تعریفونو کې د امنیت پر پوځیز اړخ ډېر ټینګار شوی دی. د دولتونو هڅې د پوځیز ځواک او وسلو د پیاوړتیا لپاره هم همدې مانا ته راګرځي. د پوځیز ځواک لوړول دا سبب ګرځي چې بهرني ګواښونه ونه شي کولای هېواد له خپل اصلي هدف څخه ـ چې هغه د ژوند بقا او د ملي ګټو پرمخ بېول دي ـ واړوي.

له هغو لومړیو کسانو څخه چې د ملي امنیت لپاره یې تعریف وړاندې کړی، والټر لیپمن، امریکایي لیکوال او څېړونکی، دی. لیپمن وایي: یو ملت هغه وخت امنیت لري چې اړ نه وي خپل مشروع منافع د جګړې د مخنیوي لپاره قرباني کړي، او که اړتیا پېښه شي، دا توان ولري چې خپل مشروع منافع د جګړې له لارې وساتي (لیپمن، ۱۹۴۳: ۵).

«یو ملت هغه مهال د امنیت څښتن بلل کېږي چې که له جګړې ځان وساتي، وکولای شي خپل بنسټیز ارزښتونه خوندي کړي، او که جګړې ته اړ شي، توان ولري چې هغه پرمخ یوسي.»

دوهم بیان: د ملي امنیت ابعاد

ملي امنیت بېلابېل ابعاد لري چې یو له بل سره نږدې تړاو لري:

سیاسي امنیت: سیاسي امنیت د هېوادونو سیاسي ثبات، د حکومتوالي سیستم، او هغه ایدیولوژي ته اشاره کوي چې حکومت ته مشروعیت ورکوي. سیاست په مختلفو معناوو کارول شوی، لکه د قدرت شدت او واک، خو زمونږ د بحث لپاره تر ټولو مناسب تعریف دا دی: د رهبري او چارو د هدایت په برخه کې د سیاست کارول، یا په بل عبارت د هېواد یا ټولنې د چارو سم مدیریت. سیاسي امنیت دا مانا لري چې سیاسي افکار او پوهې په ټولنه کې په واضح ډول شتون ولري، سیاسیون له دوه مخې او اختلاف څخه لرې وي. په عملي توګه، دا مانا لري چې هغه کسان چې د خلکو لپاره سیاسي مسایل بیانوي باید د خلکو په وړاندې امانتداري او رښتینولي ولري.

پوځي امنیت: له وستفالیایي دورې راهیسې تر وروستیو لسیزو پورې، نړیوال امنیت زیاتره په پوځي امنیت باندې تمرکز کړی و. خو نن ورځ د پوځي امنیت محوریت تر پوښتنې لاندې راغلی، او نړیوال امنیت اوس په مختلفو برخو لکه سیاسي، پوځي، اقتصادي او نورو کې تعریفېږي.

د وستفالیایي لیدلوري له مخې، امنیت محدود او تقلیل ګرا دی او له دولتونو د پولې څخه ډېر نه ټېریږي. تقلیل ګران زیاتره د دې پر ځای چې نړیوال امنیت په یوه ځانګړي مفهومي بڼه تعریف کړي، هغه د دولتونو د ملي امنیت پر تمرکز تشریح کوي. دوی حاکمیت او د هېوادونو خپلواکي د نړیوال امنیت تر ټولو مهمه برخه ګڼي.

له رئالیستي لیدلوري څخه، دولتونه د نړیوالو اړیکو اصلي لوبغاړي دي، او د دوی ترمنځ سیالي هدف یې د خپلو دولتونو پاتې کېدل دي. له همدې امله، حاکمیت او خپلواکي د دولتونو لپاره تر ټولو لوړ ارزښت لري.

په نړیوال انارشیک نظام کې هېڅ ځواک نشته چې د دولتونو پاتې کېدل تضمین کړي، او هر هېواد باید ټولې هڅې د خپلواکۍ د ساتنې لپاره وکړي، ځکه د دولت پاتې کېدل له همدې سره تړلي دي.

په پای کې، پوځي امنیت د دولتونو د وسله والو دفاعي او برید وړتیاوو پر متقابلو اغېزو او همدارنګه د هغوی د یو بل د اهدافو په درک پورې اړه لري.

اقتصادي امنیت: د شلمې پېړۍ له وروستیو لسیزو راهیسې ځینو څېړونکو استدلال وکړ چې نړۍ داسې پراو ته ننوتې ده چې پکې د امنیت اقتصادي اړخونه د سیاسي او پوځي اړخونو په پرتله زیات اهمیت مومي. د اقتصاد او امنیت ترمنځ اړیکه نوې موضوع نه ده؛ خلک تل د کاري او اقتصادي خوندیتوب په لټه کې وي، او ډېرې سیاسي ستونزې هم د اقتصادي ودې او ملي هوساینې له موضوعاتو سره تړاو لري. د نفوس زیاتوالی، د سرچینو او بازارونو ته د لاسرسي ستونزې، او فقر او محرومیت نه یوازې د هیوادونو دننه د بحران لامل ګرځي، بلکې د هېوادونو ترمنځ هم د تاوتریخوالي سبب کېدای شي. له همدې امله پیاوړی اقتصاد په خپله یوه امنیتي مسئله ګڼل کېږي، ځکه مادي او اقتصادي امکانات اساسي ارزښتونه دي چې باید وساتل او پیاوړي شي. اقتصادي امنیت په ځانګړي ډول د ډېرو مخ پر ودې هېوادونو لپاره مهم دی، ځکه دغه هېوادونه د ملي یووالي او دولت جوړونې په هڅه کې دي، حال دا چې ډېرې یې د استعماري قدرتونو د پرېکړو پر بنسټ رامنځته شوي او د قومي جوړښت او سیاسي پولو ترمنځ پوره همغږي نه لري.

ټولنیز امنیت: ټولنیز امنیت د ټولنې د بنسټونو وړتیا ته اشاره کوي چې د ژبې، کلتور، مذهب او ملي چلندونو په رامنځته کولو او ساتلو کې رول ولري. ټولنیز امنیت هغه ذهني ارامتیا او اطمینان دی چې هره ټولنه موظف ده خپلو غړو ته برابر کړي. ټولنیز امنیت عموماً په څو برخو ویشل شوی دی: دندوي یا د کار ضمینه برابرول، اقتصادي، سیاسي او قضایي امنیت. اېل ویور ټولنیز امنیت د دې توانایۍ په توګه تعریفوي چې ټولنه وکولای شي خپلې اساسي ځانګړتیاوې د بدلونونو او واقعي یا احتمالي ګواښونو پر وړاندې وساتي. ویور باور لري چې د ټولنیز امنیت تیوري د لویې کچې د ټولنیز هویت په تمرکز ولاړه ده، لکه مذهبي او قومي هویتونه، چې د دولت څخه بېل چارې او مستقلې دندې لري (خلف‌زاده او افتخاري، ۱۴۰۰: ۱۲۵–۱۲۸).

سایبري امنیت: سایبري امنیت د معلوماتي ټکنالوژۍ یوه مهمه برخه ده چې هدف یې د کمپیوټر سیستمونو، شبکو، سافټویرونو، ډیټابیسونو او نورو انټرنیټي وسایلو د معلوماتو ساتنه ده. په دې کې د معلوماتو محرمیت، بشپړتیا او د لاسرسي وړتیا تضمینول شامل دي. په بل عبارت، سایبري امنیت د هکرانو، ویروسونو، مالویر، ترهګرۍ، او هر ډول سایبري بریدونو څخه د معلوماتو او معلوماتي زیرمو خوندي ساتنه ده. د سایبري امنیت ارزښت دا دی چې په ننۍ نړۍ کې، ټولنه او اقتصاد د معلوماتي ټکنالوژۍ او شبکو پر بنسټ تکیه لري. له همدې کبله، سایبري امنیت د هر سازمان، حکومت او فرد لپاره حیاتي اهمیت لري. که سایبر سیستمونه خوندي نه وي، د مالي زیان، شخصي معلوماتو د افشا کېدو، د ملي امنیت خطر او حتی د سیاسي یا ټولنیزو ستونزو امکان زیاتېږي. او د سایبري امنیت اصلي موخې په لاندې درې برخو کې راځي:

- محرمیت : معلومات یوازې هغو کسانو ته وړاندې شي چې قانوني اجازه لري.[۱]
- بشپړتیا : معلومات د ناغوښتل شویو بدلونونو او خرابیو څخه خوندي وساتل شي.[۲]
- د لاسرسي وړتیا : سیستمونه او معلومات په اړین وخت کې د مجازو کسانو لپاره موجود وي.[۳]

درېیم مبحث: د ټکنالوژۍ او امنیت اړوند لیدلوري او نظریې

د امنیتي مسایلو په څېړنه کې، د سیاسي علومو او نړیوالو اړیکو د څېړونکو او کارپوهانو له خوا بېلابېلې نظریې وړاندې شوې دي. د امنیتي مطالعاتو له مهمو او وتلو نظریو څخه د اسلامي لیدلوري، ریښتینوالي (ریالیزم)، ازادپالنې (لیبرالیزم) او همداسی نورې نظریې او لیدلورې شتون لري. چې مونږ دلته یوازې د اسلامي لیدلوری، ریالیزم او لیبرالیزم لیدلوری سپړنه کوو.

لومړی بیان: اسلامي او ریښتینوالي (ریالیستي) لیدلوری

لمړي جز: اسلامي لیدلوري

په اسلامي لید کې امنیت یوازې د حکومت یوه اداري اړتیا نه ده، بلکې یو الهي او ټولنیز مسؤلیت ګڼل کېږي.(الذي أطعمهم من جوع وآمنهم من خوف)(قریش:۴) قرآن کریم امنیت د یوه بنسټیز نعمت په

[۱] Confidentiality
[۲] Integrity
[۳] Availability

توګه یادوي او د هغه د برابرولو دنده د اسلامي حکومت پر غاړه ږدي. له همدې امله، امنیت د ټولنیز عدالت له ستنو څخه یوه ګڼل کېږي. د نبوي سنت له مخې، په ځانګړي ډول د مدینې ټرون، امنیتي نظم د ګډ ژوند، د لږکیو د حقونو د درناوي او ټولنیز تنظیم پر بنسټ ولاړ ښیي. له نظري پلوه، د ابن خلدون اندونه د اسلامي امنیتي فکر لپاره بنسټیز ارزښت لري. هغه امنیت د مشروع واک، ټولنیز نظم او سیاسي منلو ترمنځ د اړیکې پایله بولي، او باور لري چې کورنی ثبات د بهرني امنیت شرط دی، او بې‌عدالتي او اخلاقي زوال امنیت له منځه وړي. دا لید د انسان‌محوره امنیت له نظریې سره نږدې دی، ځکه چې انسان پکې د امنیت اصلي محور دی.

په نړیوالو اړیکو کې، اسلام پر خبرو اترو، ټرونونو، ژمنو او تلپاتې سولې ټینګار کوي، او د ټپري مخالفت د نړیوال امنیت بنسټ بولي. هغه مفاهیم لکه سوله، ټرون او ګډ ژوند د اسلامي نړیوال نظم د شتون ښکارندویي کوي. د خلفاوو راشدو، په ځانګړي ډول د حضرت عمر رضي الله عنه د واکمنۍ پر مهال، د نورو ملتونو د سرحدي، رواني چاري او کلتوري امنیت ساتنې ته ځانګړې پاملرنه کېده.

په پوځیزه برخه کې هم اسلامي ښوونې ټینګار کوي چې حتی د جګړې پر مهال باید د ولسي وګړو ژوند وساتل شي او اقتصادي او کلتوري بنسټونه زیانمن نه شي. د اسلامي قومندانانو چلند جګړه د عدالت د ټینګښت وسیله بولي، نه موخه. دا لید نن سبا له اخلاقي امنیت او مشروع دفاعي نظریو سره ټراو لري.

دوهم جز؛ ریښتینوالي (ریالیزم)

د ریښتینوالي له نظره، دولت د نړیوال نظام اساسي لوبغاړی دی او ملي امنیت د قدرت له زیاتوالي سره ټراو لري. د دې لیدلوري پلویان باور لري چې نوې ټکنالوژۍ، په ځانګړي ډول مصنوعي ځیرکتیا، د دولتونو پوځي او امنیتي ځواک زیاتوي او د نړیوال رقابت بڼه بدلوي. د ریالیزم، یا واقع‌پالنې مکتب، د نړیوالو اړیکو په ډګر کې له تر ټولو مهمو فکري مکتبونو څخه ګڼل کېږي. دا مکتب، د لیبرالیزم پر خلاف ـ چې پر همکارۍ او اخلاقي ارزښتونو ټینګار کوي ـ د عیني واقعیتونو، ملي ګټو او د ځواک پر بنسټ ولاړې نړیوالې سیاست ته پام اړوي.

د واقع‌پالنې له لیدلوري، انسان یو ځان‌غوښتونکی او ګټه‌لټوونکی موجود بلل کېږي؛ له همدې امله دولتونه، چې د انسانانو له ټولګې جوړ دي، هم ځان‌محوره او ځواک‌غوښتونکي ځانګړتیاوې لري. د ریالیزم له نظره، جګړه او ټکر د نړیوال نظام طبیعي او تلپاتې پدیدې دي، ځکه چې دولتونه د ګټو د ټکر او د متقابل باور د نشتون له امله تل د بقا لپاره د خپل ځواک د پیاوړتیا هڅه کوي. واقع‌پالان باور لري چې په نړیوال نظام کې هېڅ مرکزي واک نشته، او دولتونه په داسې فضا کې ژوند کوي چې مرکزي نظم پکې نه شته. دا حالت دولتونه دې ته اړ باسي چې د خپل امنیت د ساتنې لپاره پر ځواک زیات تکیه وکړي، ځکه چې د یوه پیاوړي نړیوال بنسټ د نشتون له امله د دولتونو د بقا هېڅ ډاډ نشته. له همدې کبله، واقع‌پالان دا اند لري چې د تلپاتې سولې هڅې، او پر نړیوالو قوانینو او ټرونونو تکیه، تر ډېره خیال‌پالنه او غیر واقعي دي؛ ځکه هر دولت کولای شي د خپلو ملي ګټو د ګواښ پر مهال خپلې ژمنې له پامه وغورځوي. د ریالیزم فکري شالید د یوناني تاریخپوه توسیدیدس اثارو ته رسېږي، چې د پلوپونیز جګړو تاریخ یې لیکلی دی. هغه وایي: «عدالت یوازې د برابرانو ترمنځ مانا لري؛ پیاوړي هغه څه کوي

چې وس يې رسېږي، او کمزوري هغه څه زغمي چې اړ دي.» همدا ډول فکر د واقع‌پالنې د ليدلوري بنسټ جوړوي. نيکولو ماکياولي، توماس هابز او هاينريش فون تريچکه د ريالېزم د دوديزو (کلاسيکو) نظريه وړاندې کونکو په توګه پېژندل کېږي. هابز، د انسان د سرشت په اړه د بدبينۍ پر بنسټ او د اخلاقو او سياست د بېلتون په ټينګار سره، د «هر چا پر وړاندې د هر چا جګړې» حالت انځوروي؛ په داسې حال کې چې ماکياولي سياست د ځواک د لاسته راوړلو ډګر ګڼي او باور لري چې موخې ته د رسېدو لپاره هره وسيله د کار وړ ده.

واقع‌پالان دولت د نړيوال نظام يوازينی اصلي لوبغاړی بولي. د هغوی له انده، نا دولتي لوبغاړي لکه نړيوال سازمانونه او څو مليتي شرکتونه د دولتونو تر اغېز لاندې او د هغوی د چوکاټ په دننه کې فعاليت کوي. د ريالېزم له نظره، نړيوال نظام يو سيالي‌يز جوړښت لري چې پکې د صفر-ګټې لوبه واکمنه ده؛ يعنې د يوه دولت ګټه د بل دولت له زيان سره برابره ده. له همدې امله، واقع‌پالان په دې باور دي چې د ځواک زياتوالی د بهرنۍ پاليسۍ يو عقلاني او نه‌مخنيوی کېدونکی هدف دی. د هغوی په اند، يوازې د ځواکونو د توازن له لارې کېدای شي د يوه دولت د مطلق برلاسۍ مخه ونيول شي او له ويجاړوونکو جګړو څخه مخنيوی وشي.

د شلمې پېړۍ په نيمايي کې، او د دويمې نړيوالې جګړې تر پای وروسته، د واقع‌پالنې يوه نوې بڼه راڅرګنده شوه چې د «نوې واقع‌پالنې» يا «جوړښتي واقع‌پالنې» په نوم يادېږي. دا ليدلوری په ځانګړي ډول د دې لپاره رامنځته شو چې د نړيوالو سترو جګړو د مخنيوي په برخه کې د آرمان‌پالنې ناکامي روښانه شوه. نوې واقع‌پالان پر دې باور دي چې د ناامنۍ ريښه د انسان په سرشت کې نه، بلکې د نړيوال نظام په بې‌مرکزي جوړښت کې پرته ده. په داسې نظام کې، دولتونه د بقا لپاره اړ کېږي چې خپل ځواک زيات کړي، ځکه هېڅ داسې پورته ولاړ بنسټ نشته چې د هغوی امنيت تضمين کړي. د دې نظريې له مخې، که نړيوال نظام د کورنۍ نظام په څېر د واک يو منظم پوړيز جوړښت لرلای، د امنيت ټينګښت او د شخړو کمښت به ممکن و.

نوې واقع‌پالان په دوو ډلو وېشل کېږي: بريدکوونکی واقع‌پالان او دفاعي واقع‌پالان. بريدکوونکی واقع‌پالان باور لري چې ځينې دولتونه د خپلو جګړه‌پالو تګلارو له لارې نور دولتونه هم غبرګون ته اړ باسي. په مقابل کې، دفاعي واقع‌پالان دا نظر لري چې دولتونه د طبيعي تېري له مخې نه، بلکې د ګوابښ او له منځه تلو د وېرې له امله خپل ځواک زياتوي. په بل عبارت، د دغو دولتونو موخه بقا ده، نه پر نورو تېری.

دوهم بيان: ازادپالنه (ليبرال) ليدلوری

ليبرالي ليدلوری پر نړيوالې همکاری، بنسټونو او متقابلې ګټې ټينګار کوي او باور لري چې ټکنالوژي کولی شي د امنيت د ټينګښت سبب شي. ليبراليزم يو فکري مکتب دی چې د بېلابېلو موضوعاتو په اړه خوشبينانه ليد لري، او د امنيت موضوع ته هم له همدې ليدلوري ګوري. د ليبراليزم پلويان باور لري چې انسان په خپله سرشت کې نيک دی او تر هغه چې اړ نه شي، بد کار ته لاس نه وړي. دولتونه، چې د

انسانانو له ټولګې جوړ شوي بنسټونه دي، هم د همدې اصل تابع دي؛ يعنې دوی د تلپاتې جګړې او ټکر محکوم نه دي.

د دې مکتب له نظره، دولتونه کولای شي د دوامدارې هممنني او ګډ ژوند له لارې خپلو وګړو ته له جګړې پاک ژوند برابر کړي. د نړيوالې کچې جګړې، د ليبراليزم د پلويانو په باور، د ناسمو جوړښتونو پايله ده، او ډېر ځله دولتونه جګړې ته ورکاږل شوي دي، حال دا چې خپله يې غوښتنه نه وه. د دې مکتب پوهان په دې اند دي چې د ډيموکراتيکې سولې، له ملي پولو هاخوا همکارۍ (فراملي‌پالنې)، او بنسټيزې همکارۍ يا نهادګرايۍ له لارې کېدای شي په نړيواله کچه امنيت ټينګ شي (نجيب محمود، ۱۴۰۴: ۲۴–۲۸).

دويم څپرکی

ملي امنيت لپاره د مصنوعي ځيرکتيا فرصتونه او ننګونې

په معاصرې نړۍ کې د ټکنالوژۍ چټک پرمختګ، په ځانګړې ډول د مصنوعي ځيرکتيا وده، د بېلابېلو برخو تر څنګ د ملي امنيت په ډګر هم ژور اغېز کړی دی. مصنوعي ځيرکتيا د معلوماتو د تحليل، وړاندوينې، خارنې او پرېکړه‌نيونې په برخو کې داسې نوي امکانات رامنځته کړي دي چې د هېوادونو لپاره د امنيتي ګواښونو د مخنيوي او مديريت په برخه کې بې‌ساري فرصتونه برابروي. د همدې ټکنالوژۍ له لارې دولتونه کولای شي چې امنيتي ګواښونه په چټک او دقيق ډول وپېژني او اغېزمن غبرګون ورته وښيي.

سره له دې، مصنوعي ځيرکتيا يوازې فرصتونه نه، بلکې جدي ننګونې هم له ځان سره لري. د سايبري بريدونو زياتوالی، د معلوماتو د محرميت ستونزې، د خپلواکو وسلو کارونه، او د ټکنالوژۍ ناوړه استفاده هغه مسايل دي چې د ملي امنيت لپاره نوي ګواښونه رامنځته کوي. دا ننګونې دولتونه دې ته اړ باسي چې د مصنوعي ځيرکتيا د کارونې لپاره روښانه پاليسۍ، قانوني چوکاټونه او تخنيکي تدابير رامنځته کړي.

له همدې امله، دا څپرکی هڅه کوي چې د ملي امنيت په برخه کې د مصنوعي ځيرکتيا مهم فرصتونه او اساسي ننګونې په علمي او تحليلي ډول وڅېړي، تر څو د دې ټکنالوژۍ د اغېزو په اړه يو روښانه انځور وړاندې کړي او د اغېزمنې ګټې اخيستنې لپاره مناسبې لارې چارې روښانه کړي.

لومړی مبحث: د مصنوعي ځيرکتيا فرصتونه

مصنوعي ځيرکتيا په معاصره دوره کې د ملي امنيت په بېلابېلو برخو کې مهم فرصتونه رامنځته کړي دي. په پوځي او دفاعي برخه کې، روباټونه، خپلواک وسايل او بې‌پيلوټه الوتکې (درون) د کشف، خارنې او عملياتو په ترسره کولو کې مهم رول لري او د انساني تلفاتو کچه راکموي. همدارنګه، پنځم نسل جټ الوتکې او هوښيارې وسلې د دقيقو او چټکو پرېکړو وړتيا لري، چې د جګړې په ډګر کې ستراتيژيک برلاسی رامنځته کوي.

په روغتيايي برخه کې، مصنوعي ځيرکتيا د ټپيانو د درملنې، د ناروغيو د تشخيص او د بيړنيو حالاتو د مديريت په برخه کې مرسته کوي. په جګړه‌ييزو او کړکيچن شرايطو کې، دا ټکنالوژي کولای شي د چټکو او دقيقو طبي خدماتو د وړاندې کولو سبب شي، چې د انساني ژوند ژغورنه پياوړې کوي.

په امنيتي برخه کې، مصنوعي ځيرکتيا د ګواښونو د پېژندنې، سايبري امنيت د ټينګښت او د جرمونو د مخنيوي لپاره کارول کېږي. هوښيار سيستمونه کولای شي مشکوک فعاليتونه په چټکۍ سره تحليل کړي او د امنيتي بنسټونو د پرېکړو ملاتړ وکړي. په خارنه کې، مصنوعي ځيرکتيا د کمرې‌يي سيستمونو، مخ پېژندنې او معلوماتي تحليل له لارې د دقيقې او دوامدارې خارنې زمينه برابروي. دا چاره د عامه امنيت د ساتنې او د خطرونو د مخنيوي لپاره ګټوره ده، خو د شخصي حريم د ساتنې اړتيا هم ورسره ټرلې ده.

لومړی بیان: د پوځي او دفاعي سیستمونو پیاوړتیا

پرمختللي هېوادونه هڅه کوي چې د مصنوعي ځیرکتیا له تحلیلي ظرفیت څخه د نظامي ځواکونو د قوماندې او کنټرول په برخه کې ګټه واخلي. دغه هېوادونه د داسې متنوعو او هراړخیزو رهبرۍ او هدایت سیستمونو په جوړولو بوخت دي چې د قوماندې او پرېکړې نیولو ټولې ساحې متمرکزې کړي او د پلان جوړونې له لارې په هوایي، فضایي، سایبري، سمندري او ځمکنیو برخو کې د نظامي اقداماتو د عملي کولو زمینه برابره کړي.

په نړۍ راتلونکي کې ښایي مصنوعي ځیرکتیا د دې وړتیا ولري چې په یادو برخو کې له شته حسګرو (سینسرونو) څخه ترلاسه شوي معلومات سره یوځای کړي، تر څو د معلوماتو یو واحده سرچینه رامنځته شي. دې اقدام ته د پرېکړه کوونکو لپاره «ګډ عملیاتي انځور» ویل کېږي (کلارک، ۲۰۱۷).

اوس مهال هغه معلومات چې د پرېکړه‌کوونکو په واک کې وي، له بېلابېلو سرچینو څخه راټولېږي. دغه معلومات بېلابېل ډولونه لري او ډېرې وخت یا له یو بل سره یوځای شوي وي (ګډوالی) او یا هم له یو بل سره سمون نه خوري.د مصنوعي ځیرکتیا پر بنسټ «ګډ عملیاتي انځور» په نظري لحاظ کولای شي دا ټول معلومات په یوه واحد سکرین کې سره یوځای کړي، د خپلو او دښمنو ځواکونو یو هراړخیز او منظم انځور وړاندې کړي چې پکې هرڅه روښانه وي، او د ورودي معلوماتو انحراف او نیمګړتیاوې په اوتومات ډول اصلاح کړي. دغه ډول سیستم په پایله کې کولای شي هر حسګر (سینسر) دې ته توانمند کړي چې خپل معلومات د هرې ویشتونکې وسیلې (شلیک کوونکي) سره شریک کړي، که هغه د هر متحد یا شریک استخباراتي (اطلاعاتی)خدمت پورې تړلې وي، تر څو د هر ټاکلي هدف پر وړاندې منظم او همغږي بریدونه ترسره شي (هیچنز، ۲۰۱۹).

کېدای شي په راتلونکې کې د مصنوعي ځیرکتیا له سیستمونو څخه د هغو مخابراتي (ارتباطي)اړیکو د پېژندنې لپاره کار واخیستل شي چې د دښمن له خوا پرې شوې وي، او همدارنګه د معلوماتو د اغېزمن وېش لپاره د بدیلو لارو د موندلو په موخه ترې ګټه پورته شي. سربېره پر دې، د دغو سیستمونو د پېچلتیا له زیاتېدو سره ښایي د مصنوعي ځیرکتیا پر بنسټ الګوریتمونه وکولای شي د جګړې په ډګر کې د وخت-واقعي تحلیلونو پر بنسټ قوماندانانو ته د مناسب عملیاتي اقداماتو یوه ټولګه وړاندې کړي؛ دا کار به په بالقوه توګه د جګړې په شرایطو کې د پرېکړې نیولو کیفیت او چټکتیا دواړه ښه او لوړ کړي (دارپا، ۲۰۱۹، د امریکا دفاعي پرمختللو څېړنو اداره).

سره له دې چې په دې برخه کې لا هم څو مهم نامعلوم اړخونه موجود دي، خو د صنعت او دفاعي چارو د متخصصانو ترمنځ په دې اړه نسبي اجماع رامنځته شوې چې مصنوعي ځیرکتیا، که بشپړ انقلاب ونه بلل شي، لږ تر لږه به د خپلواکۍ (خپل پسر)او د راتلونکو جګړو پر ماهیت یو تکاملي او ژور اغېز ولري.مصنوعي ځیرکتیا د دفاعي او سایبري بریدونو وړتیاوو د پیاوړتیا لپاره د یوه بالقوه ځواک په توګه ګڼل کېږي او تمه ده چې د راتلونکي ستراتیژیک چاپېریال پر بڼې او توازن هم اغېز وکړي (احمدي و همکاران، ۱۴۰۲، ص ۵۲-۵۳).

نو ویلای شو چې مصنوعي ځیرکتیا د پوځي او دفاعي سیستمونو په پیاوړتیا کې یو مهم فرصت برابروي، ځکه دا ټکنالوژي کولای شي بېلابېل معلومات له ګڼو سرچینو څخه په منظم او یو ځای شکل سره وړاندې کړي. دا چاره د قوماندې او کنټرول بهیر اسانه کوي او پرېکړه‌کوونکو ته دا توان ورکوي چې د جګړې د ډګر یو واضح او هراړخیز انځور ولري. کله چې معلومات په یو واحد سیستم کې تحلیل او تنظیم شي، نو د پلان جوړونې بهیر ګړندی کېږي او نظامي عملیات په دقیق او همغږي ډول ترسره کېدای شي. دا ښیي چې مصنوعي ځیرکتیا د عصري جګړو د مدیریت لپاره یو اغېزناک او پرمختللی وسیله ګرځېدلی شي. همدارنګه، د مصنوعي ځیرکتیا کارونه د مختلفو نظامي برخو ترمنځ همغږي نوره هم پیاوړې کوي، ځکه هر حسګر کولای شي خپل معلومات له بېلابېلو واحدونو سره شریک کړي او په دې توګه د هدف پر وړاندې دقیق او منظم اقدام ممکن کېږي. دا ټکنالوژي نه یوازې د معلوماتو د تحلیل سرعت زیاتوي، بلکې قوماندانانو ته د وخت پر بنسټ مناسب انتخابونه هم وړاندې کوي، چې دا د پرېکړې نیولو کیفیت لوړوي. له همدې امله، ویلای شو چې مصنوعي ځیرکتیا د ملي امنیت په برخه کې یو مهم فرصت دی چې د دفاعي وړتیاوو د عصري کولو او اغېزمنتیا د زیاتوالي سبب ګرځي.

دوهم بیان: روبوټونه او خپلواکه ترانسپورتي وسایل

د مصنوعي ځیرکتیا په برخه کې راتلونکي پرمختګونه کولی شي د نړیوالو شخړو په څرنګوالي کې بدلون راولي. په ځانګړي ډول، په خپلواکو ترانسپورتي وسایلو لکه بې‌پیلوټه الوتکو، ځمکنیو وسایطو او نورو سیستمونو کې د دې ټکنالوژۍ کارول خورا اغېزمن تمامېدلی شي. پرمختللي هېوادونه اوس په پراخه کچه له مصنوعي ځیرکتیا څخه په نیمه‌خپلواکو او بشپړ خپلواکو وسایلو کې کار اخلي، چې پکې جنګي الوتکې، ځمکني وسایط او سمندري بېړۍ شاملې دي. دغه خپلواکه سیستمونه له نظري پلوه د مصنوعي ځیرکتیا ګڼې برخې رانغاړي، لکه د لید درک (بصري ادراک)، د څېړې او وینا پېژندنه، او د پرېکړې نیولو وسایل. دا ټول د دې لپاره کارول کېږي چې بېلابېل عملیات—هوایي، ځمکني او سمندري—د انسان له مستقیمې مداخلې پرته ترسره کړي.

د مصنوعي ځیرکتیا عملي کارونې په دې برخه کې د نیمه‌خپلواکو وسایطو په سوداګریزه استفاده کې هم لیدل کېږي. دا وسایل د چاپېریال د درک لپاره له مصنوعي ځیرکتیا کار اخلي، خنډونه پېژني، د حسګرو معلومات یو ځای کوي، د نقشې پر بنسټ لاره مومي، او حتی له نورو وسایطو سره اړیکه نیسي .روبوټونه او خپلواکه ترانسپورتي وسایل د مصنوعي ځیرکتیا له مهمو عملي فرصتونو څخه ګڼل کېږي چې کولای شي د پوځي او دفاعي عملیاتو ماهیت ته نوې بڼه ورکړي. د بې‌پیلوټه الوتکو، ځمکنیو وسایطو او سمندري بېړیو کارونه دا زمینه برابروي چې عملیات په لوړ دقت او چټکتیا سره، او له مستقیم انساني مداخلې پرته ترسره شي. دغه ډول سیستمونه په بېلابېلو عملیاتي چاپېریالونو کې د کار وړتیا لري او کولای شي په هم‌مهاله توګه هوایي، ځمکني او سمندري فعالیتونه پر مخ یوسي. سربېره پر دې، د مصنوعي ځیرکتیا اړوند تخنیکونه لکه بصري ادراک، د څېړو او وینا پېژندنه، او د پرېکړې نیولو هوښیار میکانېزمونه، خپلواکو وسایطو ته دا وړتیا ورکوي چې چاپېریال په دقیقه توګه درک کړي او د معلوماتو پر بنسټ مناسب اقدامات ترسره کړي. دغه وسایل د حسګرو د معلوماتو د یوځای کولو، د نقشې پر بنسټ د لارې ټاکلو،

او له نورو وسایطو سره د اړیکو د ټینګښت له لارې کولای شي عملیات په منظم او همغږي ډول مخته یوسي. له همدې امله، دا ټکنالوژي د دفاعي سیستمونو د عصري کېدو، د عملیاتو د اغېزمنتیا د لوړولو او د ستراتیژیکو موخو د ښه تحقق لپاره یو مهم فرصت برابروي.

درېم بیان : د بې‌پیلوټه الوتکو په پرمختګ کې د مصنوعي ځیرکتیا رول

د بې‌پیلوټه الوتکو (ډرونو) په صنعت کې د مصنوعي ځیرکتیا کارونه یو نوې او پرمختللې ټکنالوژي ده، چې تر ډېره د خپلواک تصمیم نیولو، د هدف پېژندنې او له هغه سره د مقابلې پر څرنګوالي راڅرخي. په بل عبارت، مصنوعي ځیرکتیا په جګړه کې ډرون ته دا توان ورکوي چې پرته له انساني مداخلې ګواښونه وپېژني، هغوی طبقه‌بندي کړي، د دوست او دښمن، او د ملکي وګړي ترمنځ توپیر وکړي، او حتی دا هم خپله وټاکي چې له هدف سره څنګه چلند وکړي. د بې‌پیلوټه الوتکو په برخه کې د مصنوعي ځیرکتیا عملي کارونه د امریکا د عملیاتو پر مهال په عراق کې څرګند شول، هلته چې اپراتوران له زرګونو کیلومترو لرې ډرونونه کنټرولول. دا الوتکې یو ټاکلی حد مصنوعي ځیرکتیا هم لري، چې له مخې یې کولای شي ځینې چارې په خپلواکه توګه ترسره کړي، لکه د الوتنې مسیر ټاکل او د عملیاتو پرمخ وړل.

په دې برخه کې د انسان او ماشین ترمنځ اړیکه هم مهمه ده. په عمومي ډول، درې ډوله حالتونه شته:

۱. نیمه‌خودکار سیستمونه: دلته ماشین چاپېریال څاري، خو اصلي پرېکړې انسان کوي.
۲. خودکار سیستمونه له نظارتي وړتیا سره: ماشین خپله عمل کولای شي، خو انسان یې څاري او که اړتیا وي مداخله کوي.
۳. بشپړ خودکار او خپلواک سیستمونه: ماشین پخپله پرېکړې کوي او انسان هېڅ کنټرول نه لري (اوزدمیر، ۲۰۱۹: ۹).

اوس مهال، په پوځي پروګرامونو کې تر ډېره لومړی او دوهم ډول کارول کېږي، لکه بې‌پیلوټه الوتکې او دقیق توغندي. مصنوعي ځیرکتیا لا تر اوسه د بشپړ خپلواک (درېیم) پړاو ته نه ده رسېدلې.د مصنوعي ځیرکتیا له مهمو کارونو څخه یو هم د ډرونونو له خوا ثبت شوو ویډیوګانو او معلوماتو تحلیل او تفسیر دی، چې مخکې به انسانانو ترسره کاوه. اوس د مصنوعي ځیرکتیا په مرسته دا پروسه چټکه او دقیقه شوې ده. همدارنګه، د (اي آي)په کارولو سره په ځینو مواردو کې د ډرون مستقیم انساني کنټرول ته اړتیا کمه شوې ده.د بېلګې په توګه، د اسرائیلو د پوځ «هارپي» ډرون نړدې یو بشپړ خودکار سیستم ته رسېدلی، چې یوازې د ځمکنۍ اپراتور له خوا پیل کېږي. همدارنګه، د امریکا «ګلوبل هواک» او «ګړي ایګل». ډرونونه هم شته، چې په پیل کې انساني لارښوونې ته اړتیا لري، خو وروسته خپله مأموریت پرمخ وړي. دا ټول د ډرونونو په برخه کې د مصنوعي ځیرکتیا د پرمختګ څرګند مثالونه دي.[1]تمه کېږي چې راتلونکي خودکار سیستمونه چې د مصنوعي ځیرکتیا پر بنسټ جوړ شوي وي، هغه کارونه به ترسره کړي چې ستړي کوونکي، خطرناک یا ککړ وي (رایان، ۲۰۱۹). دا کارونه کېدای شي د اوږدې مودې لپاره د معلوماتو راټولول او تحلیل، د کیمیاوي وسلو له ککړو سیمو پاکول، او یا د پټو چاودېدونکو توکو د موندلو لپاره د

[1] Harpy,Global Hawk,Gray Eagle

لارو څارنه شامل وي (نجات‌پوراو همکاران، ۱۳۹۸: ۲۲-۲۴).د بې‌پیلوټه الوتکو په پرمختګ کې د مصنوعي ځیرکتیا رول د معاصرو پوځي ټکنالوژیو له مهمو فرصتونو څخه شمېرل کېږي. مصنوعي ځیرکتیا ډرونونو ته دا وړتیا ورکوي چې د هدف پېژندنه، طبقه‌بندي او د مقابلې اړوند پرېکړې په خپلواکه توګه ترسره کړي. دا چاره د دې لامل ګرځي چې عملیات له لوړې کچې دقت او چټکتیا سره پرمخ ولاړ شي او د جګړې په ډګر کې د معلوماتو پر بنسټ اغېزمن اقدامات ترسره شي.سربېره پر دې، د ډرونونو په سیستمونو کې د مصنوعي ځیرکتیا کارونه د عملیاتو د اتومات کېدو کچه لوړه کړې ده، ځکه چې دا الوتکې کولای شي د الوتنې مسیر وټاکي او خپل مأموریتونه په منظم ډول پر مخ یوسي. د انسان او ماشین ترمنځ همغږي په دې برخه کې داسې تنظیم شوې چې په نیمه‌خودکار او نظارتي خودکار سیستمونو کې انسان د څارنې او لارښوونې رول لري، خو د عملیاتو ډېرى برخې د ماشین له خوا ترسره کېږي. دا وضعیت د عملیاتو د اغېزمنتیا او منظم مدیریت سبب ګرځي.همدارنګه، د مصنوعي ځیرکتیا په مرسته د ډرونونو له خوا راټول شوي معلومات او ویډیوګانې په چټک او دقیق ډول تحلیل او تفسیر کېږي، چې دا کار پخوا د انسان له خوا ترسره کېده. دغه پرمختګ د معلوماتو د پروسس سرعت زیات کړی او پرېکړه‌کوونکو ته دا امکان ورکوي چې پر وخت او پر دقیقو معلوماتو ولاړې پرېکړې وکړي. د «هارپي»، «ګلوبل هواک» او «ګرې ایګل» په څېر ډرونونه د دې ټکنالوژۍ عملي بېلګې دي، چې ښیي مصنوعي ځیرکتیا څنګه کولای شي د ډرونونو خپلواکي او د عملیاتو اغېزمنتیا لوړه کړي.په ټوله کې، د مصنوعي ځیرکتیا پر بنسټ د بې‌پیلوټه الوتکو پرمختګ دا څرګندوي چې راتلونکي سیستمونه به وکولای شي بېلابېل مهم او پېچلي مأموریتونه، لکه د معلوماتو راټولول، تحلیل او د خطرناکو سیمو څارنه، په اغېزمن او منظم ډول ترسره کړي، چې دا د ملي امنیت او دفاعي وړتیاوو د پیاوړتیا لپاره یو مهم فرصت ګڼل کېږي.

څلورم بیان: په پوځي برخه کې د مصنوعي ځیرکتیا پر بنسټ خپلواکي

مصنوعي ځیرکتیا هغه پرمختللې ټکنالوژي ده چې ماشینونو ته د معلوماتو پر بنسټ د زده‌کړې او پرېکړې کولو وړتیا وربخښي او د خپلواکو سیستمونو د رامنځته کېدو بنسټیز ځواک بلل کېږي. خپلواک سیستمونه هغه وسایل او ماشینونه دي چې کولای شي پرته له مستقیم انساني کنټرول څخه خپلې دندې ترسره کړي، او په پوځي برخه کې د دې ټکنالوژۍ له مهمو ګټو څخه شمېرل کېږي.

هغه خپلواکي چې د مصنوعي ځیرکتیا له امله رامنځته شوې، د امریکا د پخواني ولسمشر بارک اوباما د یوې مهمې پوځي ستراتیژۍ اساسي برخه وه. د دې ستراتیژۍ موخه دا وه چې د امریکا پوځ د نړیوالو سیالانو پر وړاندې خپل ټکنالوژیک برلاسی وساتي او لا پیاوړی کړي.د دندو د ډول له مخې، خپلواک سیستمونه کولای شي یا د انسان د کار وړتیا لوړه کړي او یا یې په بشپړه توګه ځای ونیسي. دا چاره انسانانو ته دا فرصت برابروي چې پر هغو پېچلو او فکري دندو تمرکز وکړي چې لوړې ذهني وړتیا ته اړتیا لري.په ټولیزه توګه، متخصصین باور لري چې پوځ له خپلواکو سیستمونو څخه ځکه زیاته ګټه اخلي چې دا

سیستمونه کولای شي هغه دندې ترسره کړي چې ستړې کوونکې، خطرناکې او چاپېریال ته زیانمنونکې وي.[۱]

عملي بېلګې: په پوځي برخه کې خپلواک سیستمونه بېلابېل عملي کارونې لري چې د جګړې د ډګر د اغېزمنتیا او خوندیتوب په لوړولو کې مهم رول لوبوي. له مهمو بېلګو څخه یې لاندې موارد یادولی شو:

۱. استخباراتي معلوماتو راټولول او شننه: خپلواک سیستمونه کولای شي د اوږدې مودې لپاره د جګړې له ډګر او شاوخوا سیمو څخه استخباراتي معلومات راټول کړي او هغه په پرله‌پسې توګه تحلیل کړي. دا سیستمونه د سنسرونو، کمرې او پرمختللو الګوریتمونو په مرسته معلومات ارزوي او قوماندانانو ته دقیق او پر وخت معلومات برابروي، چې د پرېکړې کولو بهیر چټک او اغېزمن کوي.[۲]

۲. روبوټیک وسایل او ککړ چاپېریال پاکول: روبوټیک وسایل په هغو سیمو کې کارول کېږي چې د انسان لپاره خطرناکې وي، لکه د کیمیاوي وسلو له ککړ چاپېریال سره مخ سیمې. دا وسایل کولای شي د زهري موادو د پاکولو، د ککړو توکو د راټولولو او د سیمې د خوندي کولو چارې ترسره کړي، پرته له دې چې د انسان ژوند له خطر سره مخ شي.[۳]

۳. بې‌پیلوټه وسایل او د چاودېدونکو توکو کشف: بې‌پیلوټه وسایل هغه وسایط دي چې انسان پکې شتون نه لري او له لرې واټنه یا په خپلواکه توګه کنټرولېږي. دا وسایل کولای شي لارې او سړکونه وڅېړي، مشکوکې سیمې وپلټي او د سړک غاړې سخ شوي چاودېدونکي توکي وممي. د دغو وسایلو کارول د سرتېرو د مرګ‌ژوبلې د کمولو او د عملیاتو د خوندیتوب د زیاتولو سبب ګرځي.[٤]

د دې وړتیاوو له امله، خپلواک سیستمونه د سرتېرو ژوند له خطر څخه ژغوري او همدارنګه لګښتونه کموي، ځکه چې ډېر فزیکي او ستړي کوونکي کارونه پر غاړه اخلي. ډېر شنونکي داګټې یوازې تخنیکي اړتیا نه ګڼي، بلکې دا یو تاکتیکي او ستراتیژیک ضرورت هم بولي، او ځینې یې د دې ټکنالوژۍ کارول یو اخلاقي مسؤلیت هم ګڼي، ځکه چې دا د انسان ژوند خوندي کولو کې مرسته کوي (کانګرېشنل ریسرچ سروِس، ۲۰۱۸: ۲۴–۲۵).

نو ویلای شو چې په پوځي برخه کې د مصنوعي ځیرکتیا پر بنسټ خپلواکي د معاصرو دفاعي سیستمونو له مهمو فرصتونو څخه ګڼل کېږي. مصنوعي ځیرکتیا ماشینونو ته دا وړتیا ورکوي چې د معلوماتو پر بنسټ زده‌کړه وکړي او پرېکړې ترسره کړي، چې دا کار د خپلواکو سیستمونو د رامنځته کېدو اساسي بنسټ جوړوي. دغه سیستمونه کولای شي پرته له مستقیم انساني کنټرول څخه خپلې دندې ترسره کړي، چې دا چاره د پوځي عملیاتو د چټکتیا، دقت او اغېزمنتیا د لوړولو سبب ګرځي. سربېره پر دې، خپلواک

---

[۱] Artificial Intelligence, Autonomous Systems, Third Offset Strategy, Augment, Dull, Dangerous, Dirty.

[۲] Intelligence Collection and Analysis, Surveillance, Sensors, Data Processing, Decision-Making Support.

[۳] Robotics, Chemical Contamination, Hazardous Environment, Decontamination, Toxic Materials Handling.

[٤] Unmanned Systems, Route Clearance, Explosive Detection, Improvised Explosive Devices, Remote Operation.

سیستمونه د دې وړتیا لري چې د انسان د کاري وړتیا کچه لوړه کړي او یا هم په ځینو مواردو کې د هغه ځای ونیسي. دا وضعیت انسانانو ته دا فرصت برابروي چې پر هغو پېچلو او فکري دندو تمرکز وکړي چې لوړې ذهني وړتیا ته اړتیا لري. په همدې اساس، دا ټکنالوژي نه یوازې د عملیاتو کیفیت لوړوي، بلکې د منابعو اغېزمن مدیریت هم تضمینوي.

همدارنګه، د خپلواکو سیستمونو عملي کارونې لکه د استخباراتي معلوماتو راټولول او شننه، د روبوټي وسایلو کارول په خطرناکو او ککړو چاپېریالونو کې، او د بې‌پیلوټه وسایلو له لارې د چاودېدونکو توکو کشف، دا څرګندوي چې دغه ټکنالوژي د پوځي عملیاتو په بېلابېلو برخو کې پراخ او اغېزمن حضور لري. دا سیستمونه کولای شي په دوامداره توګه معلومات راټول او تحلیل کړي، خطرناکې سیمې وڅېړي او هغه دندې ترسره کړي چې د انسان لپاره ستونزمنې یا خطرناکې وي. په پایله کې، د مصنوعي ځیرکتیا پر بنسټ خپلواک سیستمونه د سرتېرو د ژوند د خوندیتوب، د عملیاتو د مؤثریت د لوړولو او د لګښتونو د کمولو په برخه کې مهم رول لري. همدا ځانګړتیاوې دا ټکنالوژي نه یوازې یوه تخنیکي اړتیا، بلکې یو ستراتیژیک فرصت ګرځوي چې کولای شي د دفاعي وړتیاوو په پیاوړتیا کې اساسي ونډه ولري.

پنځم بیان: د مصنوعي ځیرکتیا پر بنسټ سایبري امنیتي حللارې

مصنوعي ځیرکتیا په ډېرو برخو کې بدلون راوستی، او سایبري امنیت هم له دې څخه بې برخې نه دی. د مصنوعي ځیرکتیا پر بنسټ امنیتي سیستمونه د پرمختللو الګوریتمونو او ماشین زده کړې په مرسته ګواښونه ژر پېژني او پر وړاندې یې اقدام کوي. دا سیستمونه ډېر معلومات په حقیقي وخت (کله چې یو کار یا پېښه همدا اوس وشي، سیستم یې سمدستي وګوري، تحلیل یې کړي او اقدام وکړي — نه دا چې وروسته) کې تحلیلوي او داسې نمونې او مشکوک حالتونه پیدا کوي چې ښایي د سایبري برید نښه وي. په دې ډول، سازمانونه کولی شي له مخکې ګواښونه وپېژني او مخه یې ونیسي، مخکې له دې چې لوی زیان واړوي. دا د دودیزو امنیتي سیستمونو په پرتله ښه دی، ځکه هغه اکثره یوازې په ټاکلو نښو او انساني تحلیل تکیه کوي.

د مصنوعي ځیرکتیا یوه مهمه ګټه دا ده چې ډېر کارونه په اتومات ډول ترسره کوي. دا سیستمونه په دوامداره توګه شبکه، د کارووونکو چلند، او د سیستم فعالیتونه څاري، او که کوم مشکوک حرکت ووینې، سمدستي خبرداری ورکوي. دا کار نه یوازې امنیت چټک او اغېزمن کوي، بلکې د انساني ټېروتنو امکان هم کموي. همدارنګه، مصنوعي ځیرکتیا له نوو ګواښونو زده کړه کوي او د وخت په ټېرېدو سره لا دقیق او قوي کېږي.

خو سره له دې ګټو، ځینې ستونزې هم شته. یوه مهمه اندېښنه دا ده چې بریدګر هم کولی شي له مصنوعي ځیرکتیا څخه ناوړه ګټه واخلي او داسې پرمختللي بریدونه جوړ کړي چې د عادي امنیتي سیستمونو څخه ټېر شي. بله ستونزه دا ده چې کله ناکله دا سیستمونه غلط خبرداری ورکوي، چې دا کار بې‌ځایه ستونزې رامنځته کولی شي.

له همدې امله، دا مهمه ده چې دا سیستمونه دقیق او باور وړ وي، او د انسان څارنه هم ورسره موجوده وي، څو ټولې تشې ډکې شي.په ټوله کې، د مصنوعي ځیرکتیا پر بنسټ سایبري امنیت یو ډېر مهم او

ګټور پرمختګ دی، خو باید ورسره ترلې ستونزې هم په پام کې ونیول شي. د څېړنې، پرمختګ او همکارۍ دوام به مرسته وکړي چې دا سیستمونه لا ښه شي او په راتلونکې کې قوي سایبري امنیت تأمین کړي.

د بیلګې په توګه لاندې درې مثالونه:

۱: یو بانک د مصنوعي ځیرکتیا سیستم کاروي چې د خلکو معاملې څاري. که ناڅاپه یو حساب له بل هېواد څخه لویه مشکوکه معامله وکړي، سیستم یې سمدستي بندوي او خبر ورکوي.

۲: یو شرکت کې مصنوعي ځیرکتیا شبکه څاري. که یو هکر هڅه وکړي چې سیستم ته داخل شي، دا سیستم غیر عادي حرکت تشخیصوي او حمله مخکې له زیانه دروي.

۳: ځینې هکران هم مصنوعي ځیرکتیا کاروي ترڅو داسې ایمیلونه جوړ کړي چې ډېر واقعي ښکاري . دا ایمیلونه خلک غولوي، خو بیا هم د مصنوعي ځیرکتیا امنیتي سیستمونه کولای شي دا ډول حملې وپېژني (خان، ۲۰۲۴، مخ ۱۱۱). د مصنوعي ځیرکتیا پر بنسټ سایبري امنیتي حللارې د ملي امنیت په برخه کې له مهمو فرصتونو څخه ګټه کېږي. مصنوعي ځیرکتیا د پرمختللو الګوریتمونو او ماشین زده کړې له لارې کولای شي سایبري ګواښونه په چټکۍ سره وپېژني او د هغوی پر وړاندې د مناسب غبرګون زمینه برابره کړي. د دې سیستمونو مهمه ځانګړتیا دا ده چې کولای شي په حقیقي وخت کې ډېر معلومات تحلیل کړي او هغه مشکوک فعالیتونه وموميي چې ښایي د سایبري برید نښې وي. په دې توګه، امنیتي اداري او سازمانونه کولای شي د احتمالي ګواښونو له رامنځته کېدو مخکې د مخنیوي اقدامات ترسره کړي. همدارنګه، د مصنوعي ځیرکتیا پر بنسټ امنیتي سیستمونه د شبکو، کاروونکو د فعالیتونو او د معلوماتي سیستمونو د وضعیت دوامداره څارنه کوي، چې دا کار د سایبري امنیت د چټکتیا او اغېزمنتیا سبب ګرځي. د ماشین زده کړې وړتیا دا امکان برابروي چې سیستمونه له نویو معلوماتو او پېښو څخه زده‌کړه وکړي او د وخت په تېرېدو سره د ګواښونو د پېژندنې وړتیا لا پیاوړې کړي. د بانکونو، شرکتونو او نورو ادارو په کچه د دغو سیستمونو کارول ښیي چې مصنوعي ځیرکتیا کولای شي د غیر عادي فعالیتونو په کشف، د درغلیو په مخنیوي او د سایبري بریدونو د محدودولو کې مهم رول ولوبوي.

په ټوله کې، د مصنوعي ځیرکتیا پر بنسټ سایبري امنیتي حللارې د معلوماتي زیربناوو د ساتنې، د ګواښونو د ژر پېژندنې او د امنیتي وړتیاوو د لوړولو لپاره یو مهم فرصت رامنځته کوي. دا ټکنالوژي د سایبري امنیت په برخه کې د چټک تحلیل او اتومات غبرګون وړتیا زیاتوي او د راتلونکي امنیتي چاپېریال لپاره د باور وړ حللارو د رامنځته کېدو زمینه برابروي.

شپږم بیان: سایبري جګړه

تمه کېږي چې مصنوعي ځیرکتیا به په راتلونکو کلونو کې د سایبري پوځي عملیاتو په پرمختګ کې یوه مهمه ټکنالوژي وي. اوسني سایبري امنیتي سیستمونه اکثره د پخوانیو پېژندل شوو زیانمنو کوډونو پر بنسټ کار کوي، نو هکران کولی شي د هماغو کوډونو په لږ بدلون سره له دفاعي سیستمونو تېرې وکړي. خو له بلې خوا، هغه وسایل چې په مصنوعي ځیرکتیا سمبال وي، کولای شي د شبکې د فعالیت په عمومي بڼه کې بدلونونه او غیرعادي حالتونه وپېژني. په دې توګه، دا سیستمونه کولی شي د سایبري بریدونو پر

وړاندې یو پیاوړی خنډ او دفاعي میکانیزم برابر کړي (روزنبرګ، ۲۰۱۷).سایبري جګړه د مصنوعي ځیرکتیا له هغو برخو څخه ده چې د ملي امنیت په ډګر کې د پام وړ فرصتونه رامنځته کوي. مصنوعي ځیرکتیا کولای شي د سایبري دفاعي سیستمونو وړتیا لوړه کړي، ځکه چې دا سیستمونه یوازې په پخوانیو پېژندل شوو ګواښونو تکیه نه کوي، بلکې د شبکې د فعالیتونو عمومي بڼه هم تحلیلوي او غیرعادي بدلونونه پېژندلی شي. دا وړتیا امنیتي ادارو ته اجازه ورکوي چې د سایبري بریدونو نښې په چټکۍ سره وموميي او د هغوی پر وړاندې مناسب اقدامات ترسره کړي.

همدارنګه، د مصنوعي ځیرکتیا پر بنسټ سایبري سیستمونه د معلوماتو د دوامداره تحلیل له لارې کولای شي نوي او نااشنا ګواښونه هم تشخیص کړي. دا چاره د سایبري دفاع په برخه کې د مخنیوي وړتیا پیاوړې کوي او د شبکو د ساتنې لپاره یو پرمختللی میکانیزم رامنځته کوي. په دې توګه، مصنوعي ځیرکتیا د سایبري جګړې په ډګر کې د دفاعي وړتیاوو د لوړولو او د ملي امنیت د ساتنې لپاره یو مهم تخنیکي فرصت ګڼل کېږي.

اووم بیان: ستاکسنټ عملیات

په ننني نړیوال نظام کې د ټکنالوژۍ چټک پرمختګ د امنیتي مفاهیمو بڼه بدله کړې ده. پخوا جګړې یوازې په فزیکي ډګر کې ترسره کېدې، خو اوس سایبري فضا د جګړې یو مهم ډګر ګرځېدلې ده. د دې بدلون یوه مهمه بېلګه د ستاکسنټ عملیات دي، چې د سایبري جګړې په تاریخ کې یو بېساری بدلون ګڼل کېږي او دا څرګندوي چې سایبري وسایل کولی شي فزیکي زیانونه هم رامنځته کړي.[۱] ستاکسنټ یو پرمختللی کمپیوټري خپرېدونکی پروګرام و چې په ۲۰۱۰ کال کې کشف شو. (رویترز، ۲۰۱۰)

دا زیانرسوونکی پروګرام په ځانګړي ډول د صنعتي کنټرولي سیستمونو د هدف ګرځولو لپاره جوړ شوی و او یوازې یې ځانګړي هدفونه په نښه کول. دا د هغو پروګرامونو پر وړاندې طرحه شوی و چې د فابریکو، برېښناکوټونو او اټومي تاسیساتو ماشینونه کنټرولوي، نو ځکه یې اغېز ډېر دقیق او هدفمند و.[۲] د ستاکسنټ اصلي هدف د ایران د اټومي پروګرام کمزوري کول و، په ځانګړي ډول د نطنز د یورانیمو د بډایښې تاسیسات. په دغو تاسیساتو کې سانتریفیوژونه کارول کېدل چې د یورانیمو بډایښې لپاره اړین وو. دا زیانرسوونکی پروګرام داسې طرحه شوی و چې دغه ماشینونه په پټه توګه تخریب کړي، پرته له دې چې مسؤلین پرې ژر پوه شي، او همدا پټ عمل کول یې د بریالیتوب یو مهم لامل وګرځېد.[۳]

ستاکسنټ له تخنیکي پلوه ډېر پېچلی و او په څو پراوونو کې یې فعالیت کاوه. دا د لېرد وړ حافظو له لارې هغو شبکو ته داخلېده چې له انټرنېټ څخه جلا وې، چې دا خپله د امنیتي سیستمونو د ماتولو یوه نوې لاره وه. وروسته یې د عملیاتي سیستم پټې نیمګړتیاوې کارولې او ځان یې په سیستم کې خپراوه. کله چې هدف سیستم ته ورسېد، نو لومړی یې دا ارزوله چې آیا دا سیستم د صنعتي کنټرول اړوند پروګرام لري که نه، او که یې درلود، نو بیا یې تخریبي فعالیت پیل کاوه.[۴] د دې پروګرام تر ټولو مهمه ځانګړتیا دا

---

[۱] Cyber Space، Cyber Warfare

[۲] Stuxnet، Malware، Industrial Control Systems (ICS)

[۳] Nuclear Program، Uranium Enrichment، Centrifuges

[۴] Air-Gapped Networks، Operating System Vulnerabilities

وه چې د سانتريفيوژونو سرعت يې په غير نورمال ډول بدلولو سره هغوی ته فزيکي زيان اړاوه. کله به يې سرعت لوړ کړ او کله به يې ناڅاپه راکم کړ، چې داکار د ماشينونو د خرابېدو سبب کېده. په همدې وخت کې، دا پروګرام ځان پټ ساته او د سيستم څارونکو ته يې عادي معلومات ښودل، تر څو هغوی فکر وکړي چې هر څه سم روان دي.[1]

ستاکسنټ څو ځانګړې ځانګړتياوې لرلې چې دا يې له نورو سايبري بريدونو جلا کاوه. دا لومړنی برید و چې فزيکي تخريب يې رامنځته کړ، ډېر دقيق هدف ټاکنه يې درلوده، د څو پټو تخنيکي نيمګړتياوو څخه يې ګټه اخيستې وه او پرمختللي پټ ساتونکي مېکانېزمونه يې درلودل. له همدې امله، دا د نړۍ لومړنۍ ريښتينې سايبري وسله ګڼل کېږي.[2] که څه هم هېڅ هېواد په رسمي ډول د دې عملياتو مسؤليت نه دی منلی، خو ډېرې شنونکي باور لري چې دا ډول پرمختللي عمليات يوازې د دولتونو له خوا ترسره کېدای شي، ځکه چې دا لوړ تخنيکي مهارت او پراخو سرچينو ته اړتيا لري. دا پېښه د نړيوال سياست په ډګر کې هم مهمه وه، ځکه چې دا يې وښودله چې هېوادونه کولی شي پرته له مستقيمې جګړې يو بل ته زيان ورسوي.[3]

ستاکسنټ د نړيوال امنيت پر مفهوم ژور اغېز وکړ. دا يې څرګنده کړه چې سايبري بريدونه کولی شي فزيکي زيانونه رامنځته کړي او حياتي زيربناوې لکه صنعتي سيستمونه، برېښنا او اټومي تاسيسات په نښه کړي. همدارنګه، دا پېښه د دې سبب شوه چې هېوادونه د سايبري امنيت پياوړتيا ته جدي پاملرنه وکړي(بي بي سي نيوز، ۲۰۱۰).

د ملي امنيت له نظره، ستاکسنټ څو مهم درسونه وړاندې کوي. سايبري دفاع بايد د هر هېواد د امنيتي ستراتيژۍ بنسټيزه برخه وي، د خطرونو پېژندنه او مديريت ډېر مهم دي، او د ټکنالوژۍ پرمختګ د ګواښونو پېچلتيا زياتوي. له همدې امله، هېوادونه اړ دي چې خپل امنيتي سيستمونه له نوې ټکنالوژۍ سره سم عيار کړي.

په پايله کې، ستاکسنټ عمليات د سايبري جګړې په تاريخ کې يو مهم بدلون دی. دا نه يوازې د ټکنالوژۍ ځواک څرګندوي، بلکې دا هم ښيي چې راتلونکې جګړې به تر ډېره په سايبري فضا کې ترسره کېږي. نو ځکه، د سايبري امنيت پياوړتيا د هر هېواد لپاره يوه حياتي اړتيا ګرځېدلې ده.

اتم بيان: د ملي امنيت په ساتنه کې د مصنوعي ځيرکتيا پر بنسټ څارنه

دولتي څارنه هغه وخت قانوني بڼه خپلوي چې د ملي امنيت د ساتنې په موخه وکارول شي. دا ډول نظارت د ترهګريزو بريدونو د مخنيوي لپاره په ببلابېلو بڼو ترسره کېدای شي، لکه د څارنيزو کمرېو نصبول، د انټرنېټ څارنه او د ټيليفوني اړيکو اورېدنه، تر څو اړوند معلومات راټول شي. په دې برخه کې د مصنوعي ځيرکتيا کارول کولای شي د نظارت اغېزمنتيا زياته کړي او د دوديزې انساني څارنې په پرتله پراخه جغرافيايي او معلوماتي ساحه تر پوښښ لاندې راولي. د بېلګې په توګه، د «راېون سېنټري» پروګرام چې

[1] System Manipulation، Industrial Sabotage
[2] Zero-Day Vulnerabilities، Cyber Weapon
[3] State-Sponsored Operation، Cyber Operations

د امریکا د پوځ او د هغوی د متحدو ځواکونو له لوري په افغانستان کې پلی شوی و، د مصنوعي ځیرکتیا پر بنسټ یو پرمختللی د خبرداري سیستم و. دغه سیستم د پرانیستو سرچینو معلومات، سپوږمکیز انځورونه، جغرافیایي معلومات او نور معلوماتي شاخصونه تحلیلول، څو د د بریدونو نښې وپیژني او له مخکې یې وړاندوینه وکړي.

دغه پروګرام د ۲۰۱۹ او ۲۰۲۰ کلونو ترمنځ، د ځواکونو د کمښدو په شرایطو کې رامنځته شو، هغه مهال چې د امریکا او ناټو ځواکونو غوښتل له محدودو سرچینو سره هم د امنیتي وضعیت څارنه وساتي. «راښون سښټري» وتوانېد چې د بېلابېلو معلوماتو د یوځای کولو له لارې د خطر سیمې په نښه کړي او حتی په جلال آباد کې د ۲۰۲۰ کال د جولای له لومړۍ تر دولسمې نېټې پورې د احتمالي بریدونو خبرداری ورکړي، او د مرګ ژوبلې اټکل هم وړاندې کړي. دا سیستم شاوخوا اویا سلنه دقت ته رسېدلی و او لږ تر لږه اته څلوېښت ساعته مخکې د بریدونو په اړه خبرداری ورکولای شو.[1] سربېره پر دې، دغه سیستم یوازې له نامحرمو معلوماتو څخه ګټه اخیسته، تر څو هم د ملکي انجنیرانو ګډون ممکن شي او هم معلومات له افغان شریکانو سره شریک کړل شي. دا ښیي چې څنګه کولی شي د امنیتي څارنې په برخه کې هم عملي، هم اغېزمن او هم د همکارۍ وړ لارۍ چارې وړاندې کړي (سپهر، ۲۰۲۴: ۱۰۲–۱۰۳).

له بلې خوا، د بشري حقونو د اروپایي محکمې د ۲۰۲۲ کال د راپور له مخې، دا ډول نظارتي اقدامات باید د قانوني چوکاټونو او د بشري حقونو د اصولو په رڼا کې ترسره شي، تر څو د افرادو اساسي ازادۍ تر پښو لاندې نه شي. د مصنوعي ځیرکتیا له مهمو او نورو کارونو څخه یو هم د بېپیلوټه الوتکو (ډرونونو) په ټکنالوژۍ کې د هغې کارول دي. په ځانګړي ډول، د مخ پېژندنې په سیستمونو کې د مصنوعي ځیرکتیا کارونه، او د بېپیلوټه الوتکو له لارې د خلکو لټون او څارنه، دا امکان برابروي چې ټاکل شوی کس په ډېر لوړ دقت او چټکۍ سره وپېژندل او تعقیب شي، او د تېروتنې احتمال نږدې صفر ته راکم شي (شېپارډ او نور، ۲۰۱۸: ۴۹).

پر همدې بنسټ، له هغو لارو څخه یوه چې د چین هېواد د خپلو وګړو د څارنې لپاره غوره کړې او په دې برخه کې یې پراخه پانګونه کړې، د مصنوعي ځیرکتیا او بېپیلوټه الوتکو ګډ استعمال دی. دا ترکیب، چې هم نوښتګر او هم په لومړي نظر کې لږ نااشنا ښکاري، کولای شي د معلوماتي څارنې او پېژندنې کچه په پام وړ ډول لوړه کړي، او خلک د بېپیلوټه الوتکو له لارې د مصنوعي ځیرکتیا تر دوامداره څار لاندې وساتي (ژو جیاچوان، ۲۰۱۸). نو پر دې اساس د ملي امنیت په ساتنه کې د مصنوعي ځیرکتیا پر بنسټ څارنه د امنیتي معلوماتو د راټولولو، تحلیل او د احتمالي ګواښونو د پېژندنې لپاره یو مهم فرصت ګڼل کېږي. مصنوعي ځیرکتیا کولای شي له بېلابېلو سرچینو څخه ترلاسه شوي معلومات، لکه د څارنې کمرې، سپوږمکیز انځورونه، جغرافیایي معلومات او نور معلوماتي شاخصونه، په چټکۍ سره تحلیل او یوځای

[1] State Surveillance, National Security, Counterterrorism, Surveillance Cameras, Internet Monitoring, Communications Interception, Artificial Intelligence, Raven Sentry Program, Early Warning System, Open Source Intelligence (OSINT), Satellite Imagery, Geographic Information Systems (GIS), Data Indicators, Predictive Analysis, Military Drawdown, Risk Assessment, Casualty Estimation, Accuracy Rate, Non-classified Information, Civilian Engineers, Intelligence Sharing, Security Monitoring, European Court of Human Rights, Legal Framework, Human Rights Principles.

کړي. دا وړتيا امنيتي ادارو ته دا امکان برابروي چې د ګواښونو نښې له مخکې وپېژني او د احتمالي پېښو د مخنيوي لپاره پر وخت اقدامات ترسره کړي.

د «راښون سېنټري» پروګرام بېلګه ښيي چې مصنوعي ځيرکتيا ځنګه کولای شي د محدودو سرچينو په شرايطو کې د امنيتي څارنې وړتيا لوړه کړي. د بېلابېلو معلوماتو يوځای کول او د خطرناکو سيمو تشخيص د دې سبب ګرځي چې امنيتي پرېکړې پر دقيقو معلوماتو ولاړې وي. همدارنګه، د مصنوعي ځيرکتيا کارول په بې‌پيلوټه الوتکو او د مخ پېژندنې سيستمونو کې د پېژندنې او څارنې پروسې چټکې او دقيقې کړې دي، چې د امنيتي عملياتو د اغېزمنتيا په لوړولو کې مهم رول لري. په ټوله کې، د مصنوعي ځيرکتيا پر بنسټ څارنه د ملي امنيت لپاره يو پرمختللی فرصت دی، ځکه چې دا د معلوماتو د تحليل، د ګواښونو د وړاندوينې او د امنيتي وضعيت د ښه درک کولو وړتيا زياتوي. د دې ټکنالوژۍ اغېزمن استعمال کولای شي امنيتي ادارو ته داسې وسايل برابر کړي چې د پېچلو امنيتي ننګونو پر وړاندې لا چمتو او اغېزمن اقدامات ترسره کړي.

دويم مبحث: د ملي امنيت پرواندې د مصنوعي ځيرکتيا ګواښونه او ننګونې

مصنوعي ځيرکتيا، سره له دې چې د پرمختګ مهمه وسيله ده، د ملي امنيت لپاره ځينې جدي ګواښونه هم رامنځته کوي. په ټولنيز ډګر کې د ناسمو معلوماتو او افواهاتو خپرېدل د ثبات لپاره خطر دی. په سياسي برخه کې، دا ټکنالوژي د افکارو د اغېزمنولو او مداخلې وسيله ګرځېدلی شي.په اقتصادي برخه کې، د اتومات سيستمونو له امله د کارموندنې کمښت او نابرابري رامنځته کېږي. په امنيتي او پوځي ډګر کې، سايبري بريدونه او هوښيار وسلې نوي خطرونه زېږوي.

لومړی بيان: په پوځي امنيت کې پېچلې ننګونې

نوې ټکنالوژۍ د سيال د ځواک او وړتياوو په اړه شک او بې‌باوري زياتوي. هر تخنيکي پرمختګ دا پوښتنه راولاړوي چې دا ټکنالوژي به په څه ډول وکارول شي او حقيقي اغېز به يې څومره وي. لکه ځنګه چې په دوهمه نړيواله جګړه کې خرګنده شوه، کله چې جرمني د رادار، ميخانيکي توپخانې او الوتکو په څېر نوې ټکنالوژۍ د خپل په ګټه وکارولې، نورو هېوادونو هم اړ شول چې د ټکنالوژۍ په ډګر کې سيالي پياوړې کړي.

مصنوعي ځيرکتيا د همدې مهمو تخنيکي بدلونونو له ډلې څخه ده؛ خو د جګړې په ډګر کې يې کارونه لا هم له ګنو نامعلومو اړخونو سره مل دي. تر اوسه پورې په يقيني توګه نه ده روښانه چې دا ټکنالوژي به په څه ډول وکارول شي او په جګړه کې به يې پايلې څه ښه ولري.

په تاکتيکي کچه، مصنوعي ځيرکتيا د يوه خپلواک وسلې په توګه نه، بلکې د بېلابېلو وسلو او مهمو نظامي سيستمونو د يوې برخې په توګه ادغام شوې ده. دا ټکنالوژي ټانکونو، توپخانو، الوتکو او اوبتلونو ته دا وړتيا ورکوي چې هدفونه په خپلواکه توګه وپېژني او مناسب غبرګون وښيي. تجربو ښودلې چې د مصنوعي ځيرکتيا ځينې سيستمونه آن د تمريني هوايي جګړو په سناريوګانو کې د تجربه‌کارو پوځي پيلوټانو پرتله غوره پايلې وړاندې کولی شي. سره له دې، لا هم روښانه نه ده چې دغه پرمختګونه به د جګړې ماهيت په څه ډول بدل کړي. که څه هم بېلابېل اټکلونه کېږي، خو د مصنوعي ځيرکتيا د اغېز،

برتری او عملي کارونې په اړه لا هم پراخه نامعلومتیا موجوده ده. دا وضعیت تر ډېره د دې له امله دی چې مصنوعي ځیرکتیا د وسلو، قوماندې او کنټرول له موجودو سیستمونو سره په تدریجي ډول مدغم شوې ده.

سربېره پر دې، د مصنوعي ځیرکتیا بنسټیز عناصر—لکه الګوریتمونه، معلومات او محاسباتي ځواک—په چټک او پرله‌پسې ډول وده کوي، چې دا خپله د راتلونکو پرمختګونو وړاندوینه لا ستونزمنه کوي. په پایله کې، اصلي پوښتنه دا پاتې کېږي چې سیال هېوادونه به څنګه په نوښتګرو او نه اټکل کېدونکو لارو له مصنوعي ځیرکتیا څخه ګټه واخلي، او نور هېوادونه به څنګه د دې پر وړاندې بدیلې لارې وموميي. دا به په اوږدمهال کې د ځواک یوه دوامداره او سیاله فضا رامنځته کړي (نظري، ۱۴۰۳: ۷۳). مصنوعي ځیرکتیا د پوځي امنیت په برخه کې، سره له دې چې د وړتیاوو د لوړولو فرصتونه رامنځته کوي، خو له ځینو پېچلو ننګونو سره هم مخ ده. د دې ټکنالوژۍ چټک پرمختګ د دې سبب شوی چې هېوادونه د خپلو سیالانو د تخنیکي وړتیاوو په اړه له نوو پوښتنو او اندېښنو سره مخ شي، ځکه لا تر اوسه په بشپړه توګه روښانه نه ده چې مصنوعي ځیرکتیا به په راتلونکو جګړو کې په څه ډول وکارول شي او د هغې واقعي اغېزې به څه وي. له همدې امله، د مصنوعي ځیرکتیا پراختیا د پوځي سیالۍ نوی اړخ رامنځته کوي چې هېوادونه اړ کوي خپل دفاعي او تخنیکي ظرفیتونه پیاوړي کړي.

همدارنګه، د مصنوعي ځیرکتیا د نظامي سیستمونو سره تدریجي ادغام د دې سبب شوی چې د جګړې د راتلونکي بڼې په اړه لا هم ګڼې پوښتنې موجودې وي. که څه هم دا ټکنالوژي کولای شي د وسلو، قوماندې او کنټرول سیستمونو وړتیا لوړه کړي، خو د هغې د بشپړ اغېز او راتلونکو پایلو اټکل ستونزمن دی، ځکه الګوریتمونه، معلومات او محاسبوي ځواک په دوامداره توګه وده کوي. په دې اساس، د مصنوعي ځیرکتیا په پوځي برخه کې تر ټولو ستره ننګونه دا ده چې هېوادونه باید د دې چټک بدلونونو سره ځان برابر کړي او د داسې نوښتونو پر وړاندې مناسبې لارې چارې وموميي چې د راتلونکو امنیتي سیالیو بڼه به ټاکي.

دوهم بیان : په انساني امنیت کې ننګونې

د مصنوعي ځیرکتیا او د معلوماتو د پرمختللو تحلیلي سیستمونو کارونه د امنیت په برخه کې نوې اسانتیاوې رامنځته کړې دي. د ټولنیز چلند شننه، وړاندوینه‌یي تحلیل او رقابتي ارزونه ادارو ته دا توان ورکوي چې احتمالي کورنۍ ګواښونه مخکې له مخکې وپېژني او مخه یې ونیسي. خو له دې سره سره، دا بهیر د شخصي محرمیت لپاره جدي ننګونې هم رامنځته کوي. ځکه چې دا سیستمونه تر ډېره د انسانانو پر شخصي او رفتاري معلوماتو تکیه کوي. دا کار نه یوازې د خلکو د شخصي ژوند د نقض خطر زیاتوي، بلکې کېدای شي د اجباري بازارموندنې، انتخابي بیه‌ټاکنې او د معلوماتو د ناوړه کارونې لامل هم شي.اصلي پوښتنه دا ده چې ایا شرکتونه او ادارې باید د خلکو معلومات راټول، ذخیره او وکاروي، او که دا کار تر کومه حده اخلاقي بلل کېدای شي .سربېره پر دې، د معلوماتو راایستل او ماشیني زده‌کړه په چټکۍ سره پرمختګ کوي، خو دا ټکنالوژۍ تل د محرمیت د سرغړونو او ناوړه استفادې احتمالي پایلو

ته پوره پاملرنه نه کوي. له همدې امله، دا لا هم روښانه نه ده چې کوم معلومات بايد راټول شي او کوم بايد محدود وساتل شي.

په پايله کې، دا حالت د امنيت او محرميت ترمنځ يو اساسي تضاد رامنځته کوي. له يوې خوا، معلومات د امنيت د پياوړتيا لپاره اړين دي، خو له بلې خوا، همدغه معلومات کېدای شي د سياسي ګټو لپاره وکارول شي او يا د عادي خلکو د کنټرول او ځپلو وسيله وګرځي (نظري، ۱۴۰۳: ۷۳).

د ښلګې په توګه، د امريکا د ملي امنيت ادارې له لوري د «پرېزم» څارنيز پروګرام څرګندوي چې څنګه د امنيت تر نوم لاندې د خلکو پراخ معلومات راټولېږي، چې دا کار د شخصي محرميت په اړه جدي اندېښنې راولاړوي.[1]

همدارنګه، په چين کې د ټولنيز اعتبار سيستم د خلکو چلند ارزوي او د همدې پر بنسټ هغوی ته امتيازونه يا محدوديتونه ټاکي، چې دا چاره د امنيت او فردي ازادۍ ترمنځ توازن تر پوښتنې لاندې راولي. سربېره پر دې، د «کېمبرېج انالیټیکا» قضيه، چې پکې د «فېسبوک» د کارووونکو معلومات د سياسي موخو لپاره کارول شوي وو، څرګندوي چې معلومات څنګه د خلکو پر افکارو او پرېکړو د اغېز لپاره ناوړه کارېدلی شي(کونفيسور او حکيم، ۲۰۱۸). مصنوعي ځيرکتيا د انساني امنيت په برخه کې، سره له دې چې د ګواښونو د پېژندنې او د امنيتي وړتياوو د لوړولو لپاره مهم فرصتونه رامنځته کوي، خو د شخصي محرميت او فردي ازادیو په برخه کې نوې ننګونې هم رامنځته کوي. د مصنوعي ځيرکتيا پر بنسټ تحليلي سيستمونه کولای شي د ټولنيز چلند، معلوماتو او احتمالي ګواښونو په اړه ژور تحليل ترسره کړي، خو د دې معلوماتو پراخه راټولونه د افرادو د شخصي ژوند د خوندیتوب موضوع مهمه کوي. له همدې امله، د امنيت د پياوړتيا او د خلکو د محرميت د ساتنې ترمنځ د توازن رامنځته کول يوه اساسي ننګونه ده. همدارنګه، د معلوماتو پر بنسټ د مصنوعي ځيرکتيا سيستمونو پراختيا دا پوښتنه راپورته کوي چې شخصي معلومات بايد تر کومې کچې راټول او وکارول شي. که څه هم معلومات د امنيتي پرېکړو او د احتمالي ګواښونو د مخنيوي لپاره ارزښت لري، خو ناسم استعمال يې کولای شي د افرادو د کنټرول او د شخصي ازادیو د محدودېدو سبب شي. د «پرېزم» څارنيز پروګرام، د چين د ټولنيز اعتبار سيستم او د «کېمبرېج انالیټیکا» قضيه ښيي چې د معلوماتو مديريت او د مصنوعي ځيرکتيا کارونه بايد د واضح اصولو او قانوني چوکاټونو له مخې ترسره شي، څو د امنيتي اړتياوو او انساني حقونو ترمنځ مناسب توازن وساتل شي.

درېيم بيان: ژور جعلي کاري يا جعل عميق

مصنوعي ځيرکتيا ورځ تر بلې دا وړتيا پيدا کوي چې ډېر واقعي ښکاره کېدونکي جعلي انځورونه، غږونه او ويډيوګانې جوړې کړي، چې ورته "جعل عميق" يا ډيپ فېک ويل کېږي. دا ټکنالوژي کولای شي د معلوماتي عملياتو د يوې برخې په توګه د نورو پر وړاندې وکارول شي. په حقيقت کې، جعل عميق د دروغجنو خبرې راپورونو د توليد، پر عامه افکارو د نفوذ، د خلکو د باور د له منځه وړلو، او د ډيپلوماټانو د باج‌ګيرۍ لپاره زمينه برابروي (ريمپفر، ۲۰۱۸). جعل عميق کولی شي په کوچنۍ او لويه کچه د يو هېواد

[1] NSA, PRISM Surveillance Program, Social Credit System, Cambridge Analytica, Facebook, Privacy, Security.

د ملي امنیت پر ضد وکارول شي. د بېلګې په توګه، یوه جعلي ویډیو چې د ډیپ فېک[1] له لارې جوړه شوې وي، کولای شي داسې یو ناسم پوځي اقدام وښیي چې ګواکې د ملکي وګړو پر وړاندې ترسره شوی وي. دا ټکنالوژي همدارنګه د سیاسي مشرانو لپاره ستونزې رامنځته کولی شي، لکه د ترهګرو ډلو یا جاسوسانو سره د خبرو اترو په اړه جعلي ویډیوګانې جوړول او خپرول. سربېره پر دې، جعل عمیق په حساسو وختونو کې—لکه ټاکنې یا ملي مناسبتونه—کارول کېدای شي، تر څو جعلي غږیز او انځوریز مواد تولید کړي او د ځانګړو اشخاصو او سیاسي څېرو شهرت ته زیان ورسوي.

څلورم بیان: په سایبر جګړه کې د مصنوعي ځیرکتیا خطرونه او ننګونې

مصنوعي ځیرکتیا اوس په سایبر جګړه کې دوه اړخیزه توره ده: دا هم د بې ساري فرصتونو سرچینه ده او هم د پام وړ خطرونه لري. د مصنوعي ځیرکتیا کارول په سایبر عملیاتو کې د بریدونو سرعت او دقت زیاتوي، ځکه چې پېچلي کارونه په اوتومات ډول ترسره کوي، د سیستم ضعفونه پېژني، او پلانونه په ګړندۍ او دقیقه توګه عملي کوي. خو هماغه وړتیا نوي خطرونه هم رامنځته کوي. د مصنوعي ځیرکتیا پر بنسټ بریدونه کولای شي د سافټویر ضعفونه هغه وخت وکاروي چې انسانان ځواب نه وي ورکړی، چې له دې سره د سایبر امنیت جدي زیانونه رامنځته کېدای شي. همدارنګه، د مصنوعي ځیرکتیا سیستمونو خپلواکه چلند د انساني څارنې او حساب ورکونې د نشتوالي اندېښنې راپورته کوي، چې کیدای شي د بریدونو اغېز لا زیات کړي.

یو له سترو خطرونو څخه دا دی چې مصنوعي ځیرکتیا کولای شي ډېر پرمختللي او ځان-اصلاح کوونکي بدافزارونه جوړ کړي، یعنې هغه کمپیوټري پروګرامونه چې د سیستم یا معلوماتو ته زیان رسوي. د دودیزو بدافزارونو پر خلاف، د مصنوعي ځیرکتیا پر بنسټ ګواښونه کولای شي له خپل چاپېریال څخه زده کړه وکړي، خپلې تګلارې بدلې کړي او د معمول دفاعي سیستمونو مخه ونیسي. دا وړتیا د سایبري امنیت متخصصانو لپاره دا ستونزمنوي چې بریدونه په سمه توګه اټکل او مخنیوی یې وکړي.

سربېره پر دې، مصنوعي ځیرکتیا کولای شي د سایبري جاسوسۍ لپاره وکارول شي، یعنې د حساسو معلوماتو په پټه راټولولو عمل، چې په اتومات ډول له بېلابېلو سرچینو څخه حساس معلومات راټول کړي او ملي امنیت او د شرکتونو رازونه له خطر سره مخ کړي.[2] بله اندېښنه دا ده چې د مصنوعي ځیرکتیا سیستمونه د بد نیت لرونکو کسانو له خوا کنټرول یا ناوړه وکارول شي. لکه څنګه چې مصنوعي ځیرکتیا ټکنالوژي په مهمو زیربناوو او دفاعي سیستمونو کې ننه وتلې، د سیالانو له خوا د دې ټکنالوژۍ د ناوړه ګټه اخیستنې خطر زیاتېږي. د بېلګې په توګه، مصنوعي ځیرکتیا کولای شي په بریښنا شبکه یا د اړیکو شبکې بریدونه همغږي کړي، چې پراخه ګډوډي او زیان رامنځته کړي. همدارنګه، په سایبر جګړه کې پر مصنوعي ځیرکتیا د پرېکړو کولو تکیه د دې سبب ګرځي چې که سیستمونه معلومات غلط تفسیر کړي یا ناسم حکم ورکړي، غیر ارادي پایلې رامنځته شي. دې ته اړتیا ده چې قوي امنیتي تدابیر او پروتوکولونه

[1] Deepfake
[2] Artificial Intelligence, Malware, Cyber Espionage

جوړ شي، څو د مصنوعي ځیرکتیا سیستمونه د ناوړه ګټه اخیستنې یا کمزوري کیدو څخه خوندي پاتې شي.(خان، ۲۰۲۴: مخونه ۱۱۱–۱۱۲).

د بیلګو په توګه ؛ د بانکونو د شبکې بریدونه: یو مصنوعي ځیرکتیا پر اساس ویروس کولای شي د بانکي حسابونو معلومات په څو دقیقو کې ونیسي او د کاروونکو مالي امنیت ته جدي ګواښ رامنځته کړي.

د بریښنا د شبکې ګډوډي: د مصنوعي ځیرکتیا پر بنسټ اتومات حمله کولای شي د ښار بریښنا وېش شبکه ګډوډه کړي، چې د میلیونونو خلکو ژوند او اقتصاد اغیزمن کړي.سایبر جاسوسي په شرکتونو کې: مصنوعي ځیرکتیا کولای شي د یو لوی شرکت د تولید پلانونه یا د نوي محصول رازونه راټول کړي، چې د سیال شرکتونو لپاره مالي او ستراتیژیک ګټه ولري. د مصنوعي ځیرکتیا په سایبر جګړه کې اخلاقي اړخونه هم ډېر مهم دي. د اتومات مصنوعي ځیرکتیا سیستمونو کارول په تهاجمي عملیاتو کې د حساب ورکونې او احتمالي غیر ارادي زیانونو پوښتنې راپورته کوي. د مصنوعي ځیرکتیا کارول کولی شي د جګړه کوونکو او ملکي وګړو ترمنځ کرښې ګډې کړي، چې له امله یې ښایي ملکي زیانونه رامنځته شي او اخلاقي ستونزې راپورته شي. د دې لپاره ضروري ده چې مصنوعي ځیرکتیا سیستمونه د اخلاقي لارښوونو او محافظتي میکانیزمونو سره ډیزاین شي، ترڅو خطرونه کم کړي او د نړیوالو اصولو سره مطابقت ولري. لکه څنګه چې مصنوعي ځیرکتیا پرمختګ کوي، اړینه ده چې سیاست جوړونکي، ټکنالوژي پوهان، او پوځي مشران په ګډه کار وکړي، څو دا خطرونه کنټرول کړي او داسې چوکاټونه جوړ کړي چې د سایبر جګړې کې د مصنوعي ځیرکتیا مسؤلانه کارول تضمین کړي.

درییم مبحث: د مصنوعي ځیرکتیا اغیز د ملي امنیت پر بېلابېلو ابعادو

مصنوعي ځیرکتیا د معاصر ملي امنیت یو له مهمو اغیزناکو عواملو څخه ګرځېدلې ده، ځکه چې د معلوماتو د راټولولو، تحلیل، وړاندوینې او پرېکړه‌نیونې په برخه کې نوې وړتیاوې رامنځته کوي. ملي امنیت اوس یوازې په پوځي ځواک پورې محدود نه دی، بلکې سیاسي، اقتصادي، ټولنیز، سایبري او معلوماتي اړخونه هم رانغاړي. مصنوعي ځیرکتیا په سیاسي برخه کې د حکومتولۍ او پرېکړه‌نیونې د ښه والي، په اقتصادي برخه کې د تولید او سیالۍ د زیاتوالي، او په ټولنیزه برخه کې د خدماتو د پرمختګ سبب ګرځي.

له بلې خوا، د مصنوعي ځیرکتیا ناسم استعمال کولی شي د ملي امنیت لپاره جدي ننګونې رامنځته کړي؛ لکه سایبري بریدونه، معلوماتي جګړه، د شخصي حریم نقض او د ټولنیز ثبات کمزوري کېدل. له همدې امله، د مصنوعي ځیرکتیا اغیز دوه‌ګونی ماهیت لري؛ یعنې هم د ملي امنیت د پیاوړتیا لپاره فرصتونه برابروي او هم نوي ګواښونه رامنځته کوي. په دې مبحث کې به د دې ټکنالوژۍ اغیزې د ملي امنیت پر بېلابېلو ابعادو وڅېړل شي.

لومړی بیان: سیاسي اوټولنیز اغیزې

مصنوعي ځیرکتیا د نوې ټکنالوژۍ له ډلې څخه ده چې بېلابېلې دندې لري، لکه د معلوماتو تحلیل او پروسس، د څېړې او غږ پېژندنه، پرېکړه نیول، د ژبې پوهه، سمول او نور. همدارنګه، دا ټکنالوژي کولی شي د دې ټکنالوژۍ د لرونکو (هغه څوک چې کار ورنه اخلي) لپاره هم ګټې او هم زیانونه رامنځته کړي.

مصنوعي ځيرکتيا، سره له دې چې ځينې ګټې لري لکه منطقي پرېکړه نيونه، د انساني پرېکړو د خطا کمول، په طبي چارو کې کارول او په خپلواک وسايلو کې کارول، د سياسي واکمنۍ لپاره ځينې ګواښونه هم رامنځته کړي دي. که څه هم د لېبرالیزم

د راښکاره کېدو وروسته، د عدالت، ازادۍ، هوساينې او مساواتو موضوعات د لېبرال ارزښتونو په توګه پېژندل شوي او وده يې کړې، خو نن ورځو کې دا ټکنالوژي د افرادو د محرميت او ديموکراسۍ لپاره خطرونه پېښ کړي دي. مصنوعي ځيرکتيا د ماشين په ځواک تکيه کوي او په سياسي پرېکړو کې لاسوهنه کوي، او لکه د ځينو نورو ټکنالوژيو په څېر، پرته له دې چې د بشري حقونو موضوعاتو ته پام وکړي، يوازې د ماشيني محاسبې پر اساس پرېکړې د انسان پر ځای ترسره کوي. دا ټکنالوژي پخپله کولای شي د معلوماتو آزاد خپرونه محدود کړي او د بيان ازادي په خطر کې واچوي. مصنوعي ځيرکتيا د معلوماتو راټولولو او د ځينو وختونو لپاره د ناسمو يا جانبداره (طرفدار) راپورونو جوړولو له لارې کولای شي د کورنۍ او بهرنۍ سياست په اړه د عامه افکارو په لور غلطه لار وښيي او د خلکو د فريب امکان رامنځته کړي. مصنوعي ځيرکتيا د ټولټاکنو او ديموکراتيکو مؤسسو لپاره هم ګواښونه رامنځته کړي دي. د دې ټکنالوژۍ لومړنی او مهم هدف د ديموکراتيکو ټولټاکنو (انتخابات) ګډوډول او فاسدول دی. دا کار کولای شي د فزيکي وسيلو له لارې، لکه سايبري بريدونه، او هم د رواني وسيلو په کارولو سره ترسره شي، چې په دې کې د خلکو باورونه د ټاکنو په پروسه کې مغشوش او بې باوره شي.

دوهم، بد نيت لرونکي سياسيون يا کسان کولای شي د مصنوعي ځيرکتيا څخه د ديموکراتيکو مؤسسو کمزوري کولو لپاره کار واخلي، د آزادو رسنيو او مدني ټولنې بنسټونو د کمزوري کولو له لارې خپل موخو ته ورسيږي. درېيم او تر ټولو تخريبي اغيزه يې د اساسي ارزښتونو، يعنې د قانون د تطبيق، برابري، او اقتصادي آزادۍ باندې ده. مصنوعي ځيرکتيا د ديموکراسۍ د اساسي ځانګړتياوو لکه شفافيت، ځواب ورکولو او برابري پر وړاندې مقاومت وکړي (احمدي، زرګر او آدمي، ۱۴۰۲: ۵۴–۵۵). نو ويلای شو چې مصنوعي ځيرکتيا د ملي امنيت په سياسي او ټولنيزو ابعادو کې د پام وړ اغېزې رامنځته کوي. دا ټکنالوژي د معلوماتو د تحليل، د پرېکړې نيولو او د خلکو د چلند د ارزونې له لارې کولای شي د حکومتونو او سياسي ادارو د فعاليتونو په بڼه کې بدلون راولي. له يوې خوا، مصنوعي ځيرکتيا د معلوماتو د چټک تحليل او دقيقو پرېکړو زمينه برابروي، خو له بلې خوا د سياسي واک، محرميت او د خلکو د معلوماتو د خوندیتوب په برخه کې نوې ننګونې هم رامنځته کوي.

د سياسي اړخ له مخې، مصنوعي ځيرکتيا کولای شي د عامه افکارو پر جوړېدو او د سياسي بهيرونو پر مسير اغېز وکړي. د معلوماتو د تحليل او د محتوا د توليد وړتيا دا امکان برابروي چې د خلکو نظرونه په ځانګړو لارو اغېزمن شي، چې دا چاره د ټاکنو، ديموکراتيکو بنسټونو او د معلوماتو د آزاد جريان لپاره مهمه موضوع ده. همدارنګه، په ټولنيز ډګر کې د مصنوعي ځيرکتيا کارونه د خلکو د معلوماتو راټولولو او تحليل ظرفيت زياتوي، چې د ټولنې د مديريت لپاره فرصتونه رامنځته کوي، خو د دې معلوماتو د سم او مسئولانه استعمال اړتيا هم زياتوي.

په ټوله کې، مصنوعي ځیرکتیا د سیاسي او ټولنیزو نظامونو لپاره دوه اړخیز اغېز لري؛ له یوې خوا د معلوماتو د مدیریت، پرېکړې نیونې او خدماتو د ښه والي زمینه برابروي، او له بلې خوا د محرمیت، د بیان آزادۍ او د دیموکراتیکو ارزښتونو د ساتنې په برخه کې نوې پوښتنې راپورته کوي. له همدې امله، د دې ټکنالوژۍ اغېز تر ډېره د هغې د کارونې د څرنګوالي او د قانوني او اخلاقي چوکاټونو له شتون سره تړاو لري.

دوهم بیان: اقتصادي او سایبري اغېزې

کله چې د مصنوعي ځیرکتیا پر اقتصاد او نړیوال اقتصاد د اغېزو خبرې کېږي، تحلیلګر په دې اړه په بشپړ ډول یوه ګډ نظر او باور نه لري. خو دوه ګډې پایلې څرګندې شوې دي: لومړی، د دې ټکنالوژۍ کارول د تولید او کاري وړتیا کچه لوړوي؛ او دویم، د سنتي یا دودیز دندو له منځه وړل او د نوو دندو رامنځته کول د کار په بازار کې ژور بدلونونه رامنځته کوي. سره له دې، د دې بدلونونو د توازن او اغېزو اندازه لا هم نامعلومه ده او په دې اړه بېلابېل اټکلونه شتون لري (ریکلي، ۲۰۱۸: ۳). سره له دې، کیدای شي مصنوعي ځیرکتیا پر اقتصاد او ټولنه خورا منفي اغېزې هم ولري. ځینې کارپوهان خبرداری ورکوي چې دا ټکنالوژي کولای شي د لویو شرکتونو رامنځته کېدو سبب شي — د شتمنۍ او پوهې مرکزونه — چې په انحصاري ډول پر اقتصاد منفي اغېز ولري. همدارنګه، مصنوعي ځیرکتیا کولای شي د پرمختللو (توسعه لروونکي) او پرمختیایي (د توسعې په حال کې) هېوادونو ترمنځ واټن زیات کړي، او همدارنګه مصنوعي ځیرکتیا د ځانګړو مهارتونو لرونکو کارکوونکو اړتیا لوړه کړي او په عین حال کې نور کارګران بې کاره کړي. د بیلګې په توګه په امازون شرکت کښې د انسانی کارکوونکي پرځای چې اوس اکثر ځیرک ډوبات او ماشینونه کار کوی. سربیره پردې کولای شي د کاري بازار لپاره پراخې پایلې ولري. کارپوهان همدارنګه په دې اړه خبرداری ورکوي چې دا ټکنالوژي ممکن د نابرابرۍ زیاتېدو، معاشونو کمښت، او د مالیاتو پر بنسټیزو سرچینو منفي اغېز وکړي (شچپانسکي، ۲۰۱۹). یوازې څو د ګوتو په شمېر هېوادونه به د پرمختللې مصنوعي ځیرکتیا کنټرول ولري، او دا به ژورې پایلې ولري. له یوې خوا، دغه پرمختللي هېوادونه له ټکنالوژۍ له نظره کولی شي د مصنوعي ځیرکتیا عملي ساتونکي شي او ډاډ ترلاسه کړي چې د دې پراختیا لپاره اوږدمهاله کافي منابع ځانګړي کېږي. ښایي چې مصنوعي ځیرکتیا به لا هم د لوړ مهارت لرونکو کارګرانو په ګټه وي، هغه څوک چې انعطاف، خلاقیت او قوي ستونزه حل کولو وړتیاوې لري. خو یقیناً امکان لري چې د مصنوعي ځیرکتیا سره مجهز روبوټان په تدریجي ډول د لوړ زده کړې لرونکو اشخاصو ځای ونیسي، لکه ماهر متخصصین، ډاکټران، معماران او حتی د کمپیوټر برنامه جوړونکي. راتلونکې جګړې ښایي یوازې د ځمکې، طبیعي منابعو او نفوس پورې محدوده نه وي، بلکې ممکن د بشري نسل د راتلونکي مسیر ټاکلو سبب هم شي. هغه راتلونکې چې د مصنوعي ځیرکتیا تر واک لاندې وي، ددې پرځای چې د نړیوال نابرابرۍ او فقر پر وړاندې ودریږي، ښایي د سرچینو او ځواک په یو ځای کښې تمرکز وکړي (واګنر، ۲۰۱۸).

مصنوعي ځیرکتیا ممکن د نړیوال او دولتي اقتصادي امنیت پر وضعیت هم اغېز وکړي، چې د ټولنو او نړیوالې لېبرالې نظام لپاره ډېر فرصتونه او خطرونه رامنځته کوي. وړاندوینه کېږي چې په نړۍ راتلونکې

کې هغه بدلونونه چې مصنوعي ځیرکتیا په شتمنی، هوساینې او ځواک په برخو کې رامنځته کوي، د صنعتي انقلاب یا اټومي انقلاب په پرتله ډېر ژور او پراخ به وي، ځکه چې دا به د هېوادونو دننه، نړیوالو او بهرنیو اغیزو ته هم اړوند وي. له همدې امله وړاندوینه کېږي چې تر ۲۰۳۰ کال پورې به د مصنوعي ځیرکتیا اقتصادي اغیز به شاوخوا ۱۵,۷ ټریلیونه ډالر ته ورسېږي (پي‌سي، ۲۰۱۷).

مصنوعي ځیرکتیا د دولت اقتصاد جوړونې په برخه کې یو وسیله ده او هغه عامل دی چې د نړیوال جیوپولیټیک او جیو ایکونومیک سیالۍ توازن بدلوي. د دې پر بنسټ چې یو هېواد د مصنوعي ځیرکتیا ټکنالوژۍ څخه څومره ګټه اخلي، نو ددې سره د نړیوالو اقتصادي توازنونو بدلون هم ممکن دی، چې دا بیا د هېوادونو د اقتصادي امنیت ځانګړتیاوې هم اغیزمن کولی شي. که څه هم د پرمختګ په حال کې هېوادونه د دې وسیلو د پراختیا لپاره هڅې کوي، خو په یواځې ددې کار د ترسره کولو توان نلري او ستونزو سره مخ دي. کچیري زمینه برابره شي نو مصنوعي ځیرکتیا ټکنالوژۍ منل د پرمختګ(توسعه)په حال کې هېوادونو ته د پرمختګ فرصتونه برابروي (اسیموګلو او رستریپو، ۲۰۱۹). مصنوعي ځیرکتیا کولای شي په نړدې راتلونکي کې د اقتصادي ودې پر کیفیت اغېز کولو له لارې د قدرت په توازن باندې لویې بهرني اغېزې ولري(مک‌نیل، ۱۹۸۲).مصنوعي ځیرکتیا د یوې بدلون راولوونکې اقتصادي ټکنالوژۍ په توګه د نوښت چټکتیا زیاتوي او د کار ځواک تولید لوړوي. (لو او ژو، ۲۰۱۹).

په مصنوعي ځیرکتیا باندې د سیالۍ په ډګر کې به ځینې مشران شتون ولري چې دا ټکنالوژي به په احتمالي توګه د نورو هیوادونو په پرمختګ او وړتیاوو واکمني وکړي، چې دا د نړیوالې لیبرالي اقتصادي نظم د کمزوري کېدو معنا لري (ډانزیګ، ۲۰۱۷). مخصوصاً کلچي نړي نظم څو قطبي وي لکه چین او روسیه د امریکا او غربي متحدین پر وړاندې کولي شي دواړه قطبونه د نویو تکنالوژۍ په بهیر کښې سره په سیالۍ اخته کړي.

مصنوعي ځیرکتیا د نړیوالو سیاسي لوبغاړو په لاس کې د یوې وسیلې په توګه کولی شي د دې ټکنالوژۍ د مالکانو ترمنځ بې پایدونکي(بي پای) سیالي رامنځته کړي او د هیوادونو ترمنځ ټکنالوژیکه تشه جوړه کړي. دغه ټکنالوژي، د نورو نوې رامنځته شوې ټکنالوژیو لکه د شیانو انټرنیټ، لوی ډیټا او روبوټیک په مرسته، کولی شي د تولید او توزیع په شبکو مستقیم اغیز ولري او په راتلونکې کې نوي صنعتونه رامنځته کړي. د دې ټکنالوژۍ د بې‌ساري ودې، چټک پرمختګ او نامعلومو وړاندوینو له امله د هیوادونو اقتصادي امنیت تل له خطر سره مخ وي(احمدي، زرګر او آدمي، ۱۴۰۲: ۵۶–۵۸).مصنوعي ځیرکتیا د اقتصادي او سایبري امنیت په برخو کې د ملي امنیت له مهمو اغېزناکو عواملو څخه ګڼل کېږي. د اقتصادي اړخ له مخې، مصنوعي ځیرکتیا د تولید د کچې لوړولو، د کار د موثریت زیاتولو او د نوښتونو د چټکتیا لپاره پراخ امکانات رامنځته کوي. دا ټکنالوژي کولای شي د اقتصاد په بېلابېلو برخو کې د تصمیم نیونې، تولیدي بهیرونو او خدماتو د ښه مدیریت سبب شي. له همدې امله، هغه هېوادونه چې د مصنوعي ځیرکتیا په برخه کې پرمختللي ظرفیتونه لري، کولای شي په نړیوال اقتصادي رقابت کې ځانګړی موقعیت ترلاسه کړي. له بلې خوا، د مصنوعي ځیرکتیا پراختیا د کار بازار او اقتصادي توازنونو باندې هم ژور اغېز کوي. د ځینو دودیزو دندو د کمېدو او د نوو تخصصي دندو د رامنځته کېدو له امله د کار په بازار کې بدلونونه

رامنځته کېږي. همدارنګه، هغه هېوادونه چې د دې ټکنالوژۍ د پراختیا لپاره کافي منابع، معلوماتي زیربناوې او متخصصین لري، ښایي د نورو هېوادونو په پرتله اقتصادي برتري ترلاسه کړي، چې دا حالت د نړیوالې ټکنالوژیکې او اقتصادي تشې د زیاتېدو لامل کېدای شي.

د سایبري امنیت له پلوه، مصنوعي ځیرکتیا د معلوماتي سیستمونو د ساتنې، د ګواښونو د پېژندنې او د سایبري بریدونو د تحلیل لپاره مهمه وسیله ګرځېدلې ده. خو په عین حال کې، د دې ټکنالوژۍ پر وړاندې نړیواله سیالي هم د دې سبب شوې چې هېوادونه د سایبري او تخنیکي وړتیاوو د لوړولو لپاره هڅې زیاتې کړي. په ټوله کې، مصنوعي ځیرکتیا د اقتصادي ودې، تولیدي ظرفیت او سایبري وړتیاوو د پیاوړتیا لپاره مهم فرصتونه برابروي، خو اغېز یې تر ډېره د هېوادونو د تخنیکي ظرفیت، پانګونې او د دې ټکنالوژۍ د اغېزمن مدیریت پورې تړلی دی.

درپیم څپرکی

د ملي امنیت د پیاوړتیا لپاره د نویو ټکنالوژیو د کارونې په برخه کې د دولتونو رول او تګلارې

د ملي امنیت د پیاوړتیا لپاره د نویو ټکنالوژیو کارونه د معاصر دولت د بنسټیزو مسؤلیتونو له جملې څخه شمېرل کېږي. په اوسني عصر کې، دولتونه هڅه کوي چې نوې ټکنالوژۍ په سمه او هدفمند ډول وکاروي، څو د امنیتي ګواښونو پر وړاندې اغېزمن ځواب وړاندې کړي. د دې بهیر یوه مهمه برخه د سایبري امنیت د پالیسیو جوړول دي، چې له لارې یې د معلوماتي سیستمونو ساتنه، د معلوماتو خوندیتوب او د سایبري بریدونو مخنیوی تضمینېږي. سربېره پر دې، دولتونه باید داسې لارې چارې رامنځته کړي چې د ملي امنیت د پیاوړتیا لپاره له ټکنالوژۍ څخه اعظمي ګټه پورته کړي، لکه د معلوماتو دقیق تحلیل، د استخباراتي ظرفیتونو لوړول او د چټکو پرېکړو زمینه برابرول. همدارنګه، د نویو ټکنالوژیو اغېزمنه کارونه د قانوني او اخلاقي چوکاټونو له شتون پرته ممکنه نه ده. دولتونه باید داسې قوانین او اصول وضع کړي چې د ټکنالوژۍ کارونه د بشري حقونو، محرمیت او شفافیت له اصولو سره سم تنظیم کړي. تر څنګ یې، د تخنیکي ظرفیت لوړونه، د متخصصو کادرونو روزنه او د پرمختللو زیربناوو رامنځته کول د دې سبب ګرځي چې دولتونه وکولای شي له نویو ټکنالوژیو څخه په اغېزمنه او دوامداره توګه استفاده وکړي. په دې توګه، د سمو تګلارو او قوي ظرفیتونو په مټ، نوې ټکنالوژۍ کولای شي د ملي امنیت د پیاوړتیا لپاره یو مهم او اغېزناک وسیله وګرځي.

لومړی مبحث: د نوی ټکنالوژی سمه کارونه

په معاصره نړۍ کې نوې ټکنالوژي، په ځانګړي ډول مصنوعي ځیرکتیا، د بشري ژوند په بېلابېلو برخو کې ژور بدلونونه رامنځته کړي دي. دا بدلونونه یوازې د اسانتیاوو تر کچې محدود نه دي، بلکې د دولتونو د ځواک، ملي امنیت، سیاست، اقتصاد او پوځي ظرفیتونو پر جوړښت هم مستقیم اغېز لري. له همدې امله، د دغو پرمختللو ټکنالوژیو سمه او مسوولانه کارونه یو حیاتي اصل بلل کېږي.مصنوعي ځیرکتیا د معلوماتو د تحلیل، پرېکړه‌نیونې او وړاندوینې په برخه کې بې‌ساری رول لري. په ملي امنیت کې دا ټکنالوژي د ګواښونو د پېژندنې، سایبري بریدونو د مخنیوي او استخباراتي معلوماتو د چټک تحلیل لپاره کارول کېږي. که دا سیستمونه په سمه توګه مدیریت شي، کولای شي د هېوادونو امنیتي بنسټونه پیاوړي کړي؛ خو ناسم استعمال یې د معلوماتو د افشا کېدو، ناسمو پرېکړو او حتی د امنیتي بحرانونو سبب ګرځي. په سیاسي ډګر کې، نوې ټکنالوژي د عامه افکارو پر جوړولو ژور اغېز لري. ټولنیزې رسنۍ او هوښیار الګوریتمونه کولای شي معلومات په ډېر سرعت خپاره کړي، خو په عین حال کې د ناسمې تبلیغاتي جګړې، جعلي خبرونو او افکارو د انحراف وسیله هم ګرځېدلی شي. له همدې امله، د ټکنالوژۍ کارونه باید د شفافیت، صداقت او مسوولیت له اصولو سره سم وي.

په اقتصادي برخه کې، نوې ټکنالوژي د تولید، سوداګرۍ او خدماتو بڼه بدله کړې ده. اتومات سیستمونه، ډیجیټلي بازارونه او هوښیار مدیریت د اقتصادي ودې سبب ګرځي. خو که دا بدلونونه په سمه توګه تنظیم نه شي، د کارموندنې ستونزې، اقتصادي نابرابري او د مهارتونو تشه رامنځته کولای شي. نو ځکه، اړینه ده چې هېوادونه د ټکنالوژۍ له پرمختګ سره سم خپلې اقتصادي تګلارې هم عیارې کړي.

په پوځي برخه کې، نوې ټکنالوژي لکه بې‌پیلوټه الوتکې، سایبري جګړې او هوښیار وسلې د جګړې ماهیت بدل کړی دی. دا وسایل د دقیقو عملیاتو او کم لګښت سبب ګرځي، خو که له کنټرول پرته وکارول شي، د بشري تلفاتو او نړیوالو شخړو د زیاتېدو خطر هم لري. له همدې امله، د دې ټکنالوژیو کارونه باید د نړیوالو قوانینو او اخلاقي چوکاټونو دننه وي.

لومړی بیان: د سایبري امنیت پالیسي

سایبري فضا هغه مجازي او ډیجیټلي چاپېریال دی چې زموږ ټول کمپیوټرونه، تلیفونونه، سرورونه، انټرنېټي شبکې، او د معلوماتو جریان پکې ترسره کېږي. دا فضا د فزیکي جغرافیې له محدودیتونو څخه ازاده ده او کوم څرګند سرحد نه لري. همدا ځانګړنه یې د نړیوالو اړیکو او په ځانګړي ډول د ملي امنیت لپاره یوه لویه ننګونه ګرځېدلې ده. په دې فضا کې، یو هکر چې په کابل کې ناست وي، کولای شي د نړۍ په بل سر، لکه واشنګټن یا بروکسل کې پر حساسو نظامي یا اقتصادي سیستمونو برید وکړي. په همدې ډول، یو بل بریدګر په مسکو یا بل هر ځای کې ناست، کولای شي د افغانستان د برېښنا شبکه، مخابراتي سیستمونه او یا بانکي بنسټونه له خطر سره مخ کړي.د سایبري فضا دا بې‌سرحده ماهیت دولتونه دې ته اړ کړي چې د امنیت دودیز مفاهیم له سره وارزوي. پخوا امنیت د جغرافیایي پولو، پوځونو او فزیکي دفاعي وسایلو پورې محدود و، خو نن ورځ معلومات، ډیجیټلي زیربناوې او سایبري شبکې د امنیت اصلي ستنې جوړوي. د مصنوعي ځیرکتیا راڅرګندېدل د سایبري امنیت په برخه کې یو ژور بدلون رامنځته کړی دی. دودیز امنیتي سیستمونه لکه فایروالونه، انټي‌وایرس پروګرامونه او د لاسلیک پر بنسټ کشف کوونکي، یوازې هغه ګواښونه پېژني چې مخکې ثبت شوي وي. دا سیستمونه د یوه دودیز ساتونکي په څېر دي چې یوازې هغه مجرم پېژني چې مخکې یې لیدلی وي. خو مصنوعي ځیرکتیا د یو پرمختللي او هوښیار څارونکي په څېر عمل کوي، چې د چلند نمونې تحلیلوي او کولای شي حتی نوې او ناپېژندل شوې حملې هم کشف کړي.

الف. د مصنوعي ځیرکتیا په مرسته د ګواښونو څارنه او تشخیص؛ د سایبري امنیت په برخه کې د مصنوعي ځیرکتیا تر ټولو مهمه ونډه د غیرعادي چلند کشف دی. دودیز سیستمونه د "لاسلیکونو" پر بنسټ کار کوي، یعنې د هر مالویر لپاره یو ځانګړی ډیجیټلي نښه لري. خو په معاصره نړۍ کې، بریدګر په دوامداره توګه خپل تخنیکونه بدلوي او هره ورځ نوي مالویرونه تولیدوي، چې له امله یې د لاسلیک پر بنسټ سیستمونه ډېر ژر زاړه کېږي.[1]

مصنوعي ځیرکتیا، په ځانګړې توګه د ماشین زده کړې الګوریتمونه، کولای شي د شبکې د عادي چلند یوه بنسټیزه نمونه جوړه کړي. دا سیستمونه د وخت په تېرېدو سره زده کړه کوي چې کوم فعالیتونه عادي دي او کوم غیرعادي. کله چې یو فعالیت له دې نمونې څخه انحراف وکړي، سیستم سمدستي خبرداری ورکوي.[2]

[1] Anomaly Detection
[2] Machine Learning,Baseline

د بېلګې په توګه، که د يوې پوځي اډې په شبکه کې يو کارونکی عموماً د ورځې له ۸ بجو تر ۵ بجو پورې کار کوي، خو ناڅاپه د شپې په ۲ بجو له هغه حساب څخه د حساسو معلوماتو ډاونلوډ پيل شي، نو مصنوعي ځيرکتيا دا عمل د خطر په توګه پېژني. دا تحليل يوازې د وخت پر بنسټ نه دی، بلکې د موقعيت، د لاسرسي ډول، د معلوماتو حجم او د کارووونکي د تېرو کړنو پر بنسټ ترسره کېږي.

په نړيواله کچه، د مصنوعي ځيرکتيا پر بنسټ امنيتي سيستمونه لکه د "خپل‌زده کوونکي شبکې ساتونکي" د پام وړ پرمختګ کړی دی. دا ډول سيستمونه د انسان د معافيتي سيستم په څېر کار کوي، يعنې لومړی "عادي حالت" زده کوي او بيا هر ډول "ناروغي" يا غيرعادي فعاليت تشخيصوي.[1]

د افغانستان په څېر هېواد کې، چې امنيتي ګواښونه يې لوړ دي او تخنيکي امکانات يې محدود دي، دا ډول ټکنالوژي کولای شي حياتي رول ولوبوي. د بېلګې په توګه، که د برېښنا د وېش شبکه يا د مخابراتو مرکزي سيستم د مصنوعي ځيرکتيا پر بنسټ څارنه ولري، نو د احتمالي سايبري بريدونو مخنيوی به په وخت سره ممکن شي.

ب. اتوماتيک غبرګون او چټک دفاعي اقدامات؛ د سايبري امنيت په ډګر کې، يوازې د برېد کشف کول کافي نه دي، بلکې چټک او پر وخت غبرګون هم حياتي ارزښت لري. په ډېرو مواردو کې، که غبرګون ځنډېږي، نو برېد کوونکی کولای شي په څو دقيقو يا حتی ثانيو کې لوی زيان واړوي.

مصنوعي ځيرکتيا دا وړتيا لري چې په اتومات ډول دفاعي اقدامات ترسره کړي. دا اقدامات کېدای شي لاندې موارد شامل کړي:

۱ - د شکمن ای پي پته بندول.[2]

۲ - د اخته شوي کارونکي حساب غير فعالول

۳ - د برېد لاندې سرور له شبکې څخه جلا کول

۴- د معلوماتو جريان خوندي چينل ته اړول

د اتوماتيک غبرګون ګټه دا ده چې د انساني ځنډ مخه نيسي. خو له دې سره سره، خطرونه هم لري. که سيستم په تشخيص کې تېروتنه وکړي، نو کېدای شي يو عادي فعاليت د ګواښ په توګه وپېژني او مهم خدمات وځنډوي.

له همدې امله، د "انسان-په-حلقه" اصل ډېر مهم دی. په دې ميکانيزم کې، حساس سيستمونه لکه روغتونونه، برېښنا شبکې او پوځي تاسيسات د بشپړ اتومات پر ځای نيمه‌اتومات سيستم کاروي، چې وروستی پرېکړه يو انساني متخصص کوي.[3]

---

[1] Self-learning Cyber Defense Systems

[2] «د شکمن IP پته بندول» معنا دا ده چې يو ځانګړی انټرنېټي IP (هغه عددي پته چې وسيله يې په انټرنېټ کې پېژني) د امنيتي دلايلو له مخې بند يا محدود کېږي تر څو نور د شبکې يا ويب‌سايټ ته لاسرسی ونه لري.

[3] Human-in-the-Loop

ج. عامه-خصوصي همکاري ؛ په معاصره نړۍ کې، د سايبري امنيت بار يوازې دولت نشي پورته کولای. د نړۍ ډېر پرمختللي ټکنالوژيکي شرکتونه د مصنوعي ځيرکتيا په برخه کې مخکښ دي او پراخ معلوماتي سرچينې لري. له همدې امله، د دولت او خصوصي سکتور ترمنځ همکاري حياتي ارزښت لري.[1]

په دې همکارۍ کې:

۱- شرکتونه نوي سايبري ګواښونه له دولت سره شريکوي

۲- دولت استخباراتي معلومات له شرکتونو سره تبادله کوي

۳-ګډې څېړنې او تخنيکي پروژې ترسره کېږي

خو دلته د محرميت او امنيت ترمنځ تعادل يو مهم بحث دی. شرکتونه د خپلو کارونکو د معلوماتو ساتنه کوي، خو دولتونه د ملي امنيت مسؤليت لري. د دې ستونزې د حل لپاره، د معلوماتو "ناپېژند کول"يو اغېزمنه لاره ده، چې پکې د افرادو پېژندګلوي لرې کېږي خو معلوماتي ارزښت پاتې کېږي.[2]

د افغانستان لپاره، دا اړينه ده چې له مخابراتي او ټکنالوژيکي شرکتونو سره رسمي چوکاټونه جوړ شي، څو د معلوماتو تبادله په قانوني او خوندي ډول ترسره شي.

د سايبري امنيت پنځه‌پړاويزه چوکاټ

د سايبري امنيت لپاره يو منظم چوکاټ اړين دی. دا چوکاټ لاندې پړاوونه لري:

۱. پېژندنه : د مهمو شتمنيو او کمزوريو معلومول

۲. ساتنه : د دفاعي تدابيرو پلي کول

۳. کشف : د ګواښونو پر وخت پېژندنه

۴. غبرګون : د برېد پر وړاندې اقدام

۵. بيارغونه : د سيستم بېرته عادي کول.[3]

دا چوکاټ دولتونو ته دا توان ورکوي چې سايبري امنيت په منظم او سيستماتيک ډول مديريت کړي، او د راتلونکو ګواښونو لپاره چمتو واوسي.

دوهم بيان: د مصنوعي ځيرکتيا قانوني او اخلاقي چوکات

د مصنوعي ځيرکتيا چټک پرمختګ په معاصره نړۍ کې ژور بدلونونه رامنځته کړي دي. دا ټکنالوژي نه يوازې د اقتصاد، امنيت او اداري په برخو کې د پرمختګ سبب ګرځي، بلکې له ځان سره ګڼ شمېر حقوقي او اخلاقي ننګونې هم راوړي. که چېرې د مصنوعي ځيرکتيا کارونه د مناسب قانوني او اخلاقي چوکاټ له شتون پرته ترسره شي، نو دا به د يوې داسې ځواکمنې وسيلې په څېر وي چې کنټرول يې ستونزمن وي او ناوړه پايلې رامنځته کولای شي. له همدې امله، د دولتونو لپاره اړينه ده چې د دې ټکنالوژۍ د کارونې لپاره واضح، منظم او عملي چوکاټونه رامنځته کړي. قانوني چوکاټ د دې لپاره جوړېږي چې د مصنوعي ځيرکتيا کارونه تنظيم کړي، مسؤليتونه مشخص کړي، او د سرغړونو په صورت

[1] Public-Private Partnership
[2] Data Anonymization
[3] Identify,Protect,Respond,Detect,Recover

کې د حساب ورکونې زمینه برابره کړي. په اوسني وخت کې، ډېرى قوانین د دودیزو ټکنالوژیو لپاره جوړ شوي او د مصنوعي ځیرکتیا پیچلي ماهیت ته په بشپړه توګه ځواب نه شي ویلای. د بېلګې په توګه، که یو خودکار موټر پېښه وکړي، دا لا هم روښانه نه ده چې مسؤلیت به د موټر پر مالک وي، که د سافټویر پر جوړونکي، او که د هغه شرکت پر غاړه چې سیستم یې فعال کړی دی. دا ډول حقوقي ابهامات ښیي چې د مصنوعي ځیرکتیا لپاره ځانګړي قوانین اړین دي. له بلې خوا، اخلاقي چوکاټ د قانوني چوکاټ بشپړونکی ګڼل کېږي. هر هغه څه چې قانوني وي، لازماً اخلاقي نه وي. مصنوعي ځیرکتیا کولای شي داسې پرېکړې وکړي چې د قانون له مخې سمې وي، خو د عدالت، انصاف او بشري کرامت خلاف وي. د بېلګې په توګه، یو استخدامي سیستم چې د مصنوعي ځیرکتیا پر بنسټ کار کوي، ممکن د معلوماتو پر اساس ښځې یا یو ځانګړی ټولنیز ګروپ کم انتخاب کړي. دا کار ښایي قانوني ستونزه ونه لري، خو اخلاقي ستونزه لري، ځکه تبعیض رامنځته کوي.

مصنوعي ځیرکتیا تر ډېره پر معلوماتو ولاړه ده، او دا معلومات اکثر د خلکو له شخصي ژوند سره تړاو لري. د معلوماتو ناسم استعمال کولای شي د خلکو د محرمیت او ازادۍ جدي نقض ته لاره هواره کړي. د بېلګې په توګه، د مخ پېژندنې سیستمونه که بې له قانوني چوکاټه وکارول شي، کولای شي د خلکو دوامداره څار ممکن کړي، چې دا به د بیان ازادي محدوده کړي او د دولت او خلکو تر منځ باور کمزورى کړي. له همدې امله، د معلوماتو د ساتنې لپاره واضح اصول، لکه د رضایت اخیستل، د معلوماتو محدود استعمال، او د سرغړونو په صورت کې خبرتیا، ډېر مهم دي.

بله مهمه موضوع شفافیت یا روښتیا ده. د مصنوعي ځیرکتیا ډېرى سیستمونه د "تور بکس" په ډول کار کوي، یعنې پایلې وړاندې کوي خو د پرېکړو منطق یې څرګند نه وي. دا حالت د اعتماد د کمښت لامل ګرځي. که یو سیستم د یو کس د پور غوښتنلیک رد کړي، خو دلیل یې واضح نه کړي، نو دا کار د عدالت خلاف ګڼل کېږي. له همدې امله، د تشریح کېدونکي مصنوعي ځیرکتیا مفکوره رامنځته شوې ده، چې موخه یې دا ده چې سیستمونه د خپلو پرېکړو وضاحت وړاندې کړي.

د عدالت او تعصب موضوع هم په دې برخه کې ډېر اهمیت لري. مصنوعي ځیرکتیا د هغو معلوماتو پر بنسټ زده کړه کوي چې ورته ورکول کېږي. که معلومات تعصب ولري، نو پایلې به هم تعصب لرونکې وي. د بېلګې په توګه، که یو امنیتي سیستم د یو خاص قوم یا سیمې خلکو ته د شک په سترګه وګوري، نو دا به بې‌عدالتي زیاته کړي او ټولنیز بې‌ثباتي به رامنځته کړي. له همدې امله، د معلوماتو د کیفیت او توازن تضمین اړین دی.

یو بل مهم بحث د ملي امنیت او فردي ازادۍ ترمنځ توازن دی. دولتونه هڅه کوي چې د مصنوعي ځیرکتیا له لارې امنیت ټینګ کړي، خو که دا کار بې له محدودیته ترسره شي، نو د خلکو ازادۍ به تر فشار لاندې راشي. د بېلګې په توګه، د ترهګرۍ د مخنیوي لپاره د معلوماتو څار کولای شي ګټور وي، خو که دا څار بې‌حده شي، نو د خلکو شخصي حریم ته زیان رسوي. نو ځکه، قانوني چوکاټ باید داسې تنظیم شي چې هم امنیت وساتي او هم ازادۍ خوندي کړي.

همدارنګه، مصنوعي ځیرکتیا یو نړیوال ماهیت لري او سرحدونه نه پیژني. یو سیستم کېدای شي په یو هېواد کې جوړ شي او په بل کې وکارول شي. له همدې امله، نړیوال معیارونه او همغږي ضروري ده. که په یو هېواد کې سخت قوانین وي او په بل کې نه وي، نو شرکتونه کولای شي له کمزورو قوانینو ځخه ناوړه استفاده وکړي.

د افغانستان په شرایطو کې، که څه هم مصنوعي ځیرکتیا لا هم په لومړیو مرحلو کې ده، خو بیا هم د قانوني او اخلاقي چوکاټ جوړول ډېر مهم دي. په افغانستان کې د قوانینو د تطبیق کمزوري، د تخنیکي ظرفیت نشتوالی، او د عامه پوهاوي کموالی هغه ننګونې دي چې باید ورته جدي پاملرنه وشي. د دې لپاره اړینه ده چې د معلوماتو د ساتنې لپاره ځانګړی قانون جوړ شي، د مصنوعي ځیرکتیا ملي ستراتیژي رامنځته شي، تخنیکي ظرفیتونه لوړ شي، او نړیوالو همکاریو ته وده ورکړل شي.

په پایله کې، ویلای شو چې مصنوعي ځیرکتیا یو دوه مخی ټکنالوژي ده چې هم فرصتونه لري او هم خطرونه. که دا ټکنالوژي د قانوني او اخلاقي چوکاټ لاندې مدیریت شي، نو کولای شي د ملي امنیت، اقتصادي پرمختګ او ټولنیز عدالت لپاره ګټوره تمامه شي. خو که بې کنټروله پاتې شي، نو د بشري حقونو نقض، بې‌عدالتي او سیاسي بې‌ثباتي رامنځته کولای شي. له همدې امله، دولتونه باید د پرمختګ ترڅنګ د کنټرول لپاره هم قوي میکانیزمونه رامنځته کړي.

درېیم بیان : د مصنوعي ځیرکتیا د اخلاقي کارونې پالیسي

لکه څنګه چې مصنوعي ځیرکتیا په چټکۍ سره پرمختګ کوي، د دې ټکنالوژۍ کارول په بېلابېلو برخو کې مهمې اخلاقي ستونزې راولاړوي. د مصنوعي ځیرکتیا ادغام (یوې ټکنالوژۍ د نورو سیستمونو سره یوځای کول) باید د داسې پالیسیو (اصولو او مقرراتو) له مخې ترسره شي چې دا ټکنالوژي په اخلاقي ډول او د ټولنې له ارزښتونو سره سم وکارول شي. دغه پالیسۍ باید مهم موضوعات لکه عدالت، رونټیا، حساب ورکونه او د فردي حقونو ساتنه په پام کې ونیسي. که یو قوي اخلاقي چوکاټ موجود نه وي، نو مصنوعي ځیرکتیا کولای شي نابرابري زیاته کړي، ناعادلانه اړخنیوی پیاوړی کړي او د خلکو باور کمزوری کړي.[1]

د عدالت او برابرۍ تضمین: یو له مهمو اصولو څخه دا دی چې عدالت او برابري ،له ټولو خلکو سره عادلانه او یو شان چلند تضمین شي. مصنوعي ځیرکتیا کله ناکله د هغو معلوماتو له امله چې پرې روزل شوې وي، تعصب (ناانصافه لېوالتیا) زیاتولی شي. له همدې امله، پالیسۍ باید دا یقیني کړي چې سیستمونه په سمه توګه وازمویل شي، څو دا ډول ستونزې وپېژندل شي او حل شي. همدارنګه، د سیستمونو په جوړولو کې باید بېلابېل خلک او متخصصین ګډون ولري، څو مختلف نظرونه پکې شامل شي او د تعصب کچه راکمه شي. دا ډېره مهمه ده چې مصنوعي ځیرکتیا د ټولنې ټولو خلکو ته په عادلانه ډول خدمت وکړي.[2]

---

[1] Integration, Policies
[2] Fairness, Equity

روښتیا او حساب ورکونه: روښتیا یعنې معلومات په څرګند او واضح ډول وړاندې کول او حساب ورکونه ،یعنې د پرېکړو مسؤلیت منل. د مصنوعي ځیرکتیا په اخلاقي کارونه کې ډېر مهم اصول دي. پالیسۍ باید بنسټونه او سازمانونه دې ته وهڅوي چې په روښانه ډول څرګنده کړي چې مصنوعي ځیرکتیا څنګه پرېکړې کوي، کوم معلومات کاروي او کوم محاسبوي اصول (الګوریتمونه) پکې کارول کېږي.

دا کار خلکو ته دا امکان برابروي چې د سیستم پرېکړې درک کړي او ارزونه یې وکړي. همدارنګه، باید داسې میکانیزمونه موجود وي چې که څوک د مصنوعي ځیرکتیا له امله زیان وویني، وکولای شي خپل شکایت ثبت کړي او خپل حق ترلاسه کړي. سربېره پر دې، باید منظمې ارزونې او تفتیشونه (یعنې د سیستمونو بیاکتنه) ترسره شي، څو ډاډ ترلاسه شي چې اخلاقي اصول په دوامداره توګه مراعات کېږي.[1]

د محرمیت ساتنه او امنیت: د محرمیت ساتنه، یعنې د شخصي معلوماتو خوندیتوب، او امنیت د مصنوعي ځیرکتیا په کارونه کې ډېر مهم اصول دي. دا سیسټمونه د زیاتو شخصي معلوماتو کارولو ته اړتیا لري، چې له همدې امله د معلوماتو د خوندیتوب په اړه جدي اندېښنې رامنځته کېږي.

پالیسۍ یا اصول او مقررات باید دا تضمین کړي چې معلومات په خوندي ډول وساتل شي، لکه د معلوماتو کوډ کول او بې‌نومه کول. همدارنګه، اړینه ده چې خلکو ته په روښانه ډول څرګنده شي چې معلومات څنګه راټولېږي او د هغوی رضا یا موافقه تر لاسه شي.سربېره پر دې، باید د مصنوعي ځیرکتیا سیسټمونه داسې طرحه او جوړ شي چې د هک کېدو او ناوړه کارونې مخه ونیسي، څو د خلکو بنسټیز حقونه خوندي پاتې شي او د ټکنالوژۍ پر وړاندې باور پیاوړی شي (خان، ۲۰۲۴: ۱۱۷–۱۱۸).د محرمیت ساتنه او امنیت د مصنوعي ځیرکتیا د مسؤلانه کارونې له اساسي شرطونو څخه دي. ځکه چې د مصنوعي ځیرکتیا ډېرې سیستمونه د فعالیت لپاره د پراخو معلوماتو راټولولو او تحلیل ته اړتیا لري، نو د شخصي معلوماتو د خوندي ساتنې موضوع ځانګړې اهمیت پیدا کوي. د معلوماتو ناسم مدیریت کولای شي د افرادو د محرمیت حقونه له خطر سره مخ کړي، له همدې امله اړینه ده چې د معلوماتو د ساتنې لپاره روښانه اصول او مقررات موجود وي.

همدارنګه، د معلوماتو کوډ کول، بې‌نومه کول او د معلوماتو د راټولولو په اړه د خلکو خبرول هغه لارې چارې دي چې د مصنوعي ځیرکتیا پر سیستمونو د باور د زیاتېدو سبب ګرځي. د خلکو رضا او پوهاوی د دې ټکنالوژۍ د قانوني او اخلاقي کارونې لپاره مهم اصل بلل کېږي. سربېره پر دې، د مصنوعي ځیرکتیا سیستمونه باید له امنیتي پلوه داسې جوړ شي چې د سایبري بریدونو او ناوړه استفادې پر وړاندې مقاومت ولري. په ټوله کې، د محرمیت ساتنه او امنیت یوازې تخنیکي موضوع نه ده، بلکې د مصنوعي ځیرکتیا د پراختیا یو حقوقي او اخلاقي اړخ هم دی. که د معلوماتو د خوندیتوب لپاره مناسب میکانیزمونه رامنځته شي، نو مصنوعي ځیرکتیا کولای شي د خلکو باور وساتي او په خوندي او اغېزمن ډول د ټولنې او ملي امنیت په خدمت کې وکارول شي.

[1] Transparency, Accountability, Policies, Algorithms, Audits

دوهم مبحث: د ملي امنيت د پياوړتيا لارى

په معاصره نړۍ کې ملي امنيت يو څو اړخيز مفهوم دى چې يوازې په پوځي ځواک پورې محدود نه دى، بلکې سايبري امنيت، معلوماتي کنټرول، تخنيکي پرمختګ، او نړيوال تعاملات ټول پکې مهم رول لري. د مصنوعي ځيرکتيا (اى آى) پراختيا د دې سبب شوې چې د امنيت بڼه بدله شي او دولتونه اړ کړي چې خپل امنيتي ستراتيژي د نوې ټکنالوژۍ سره سم عيار کړي. د ملي امنيت د پياوړتيا لپاره درې اساسي برخې ډېر اهميت لري: تخنيکي ظرفيت لوړونه، نړيواله همکاري، او د ګواښونو مديريت لپاره ستراتيژي.

لومرى بيان: تخنيکي ظرفيت لوړونه

د معاصر نړيوال نظام په چوکاټ کې، تخنيکي ظرفيت د ملي امنيت يو له اساسي او ټاکونکو عناصرو څخه ګڼل کېږي. پخوا به امنيت تر ډېره د پوځي ځواک، سرټېرو شمېر او وسلو پورې تړلى و، خو نن ورځ دا مفهوم د بنسټيز بدلون سره مخ شوى دى. اوس امنيت تر ډېره د معلوماتي ټکنالوژۍ، سايبري فضا، مصنوعي ځيرکتيا ، او پرمختللو تحليلي سيستمونو پورې تړاو لري. هغه هېوادونه چې په دې برخو کې پرمختللي وي، نه يوازې خپل داخلي امنيت تأمينوي، بلکې په نړيواله کچه هم ستراتيژيک برلاسى ترلاسه کوي (ډانزيګ، ۲۰۱۷).

مصنوعي ځيرکتيا په ځانګړې توګه د تخنيکي ظرفيت د لوړولو په برخه کې مرکزي رول لري. دا ټکنالوژي کولاى شي د لويو معلوماتو (لويه ډيټا) تحليل په ډېر چټک او دقيق ډول ترسره کړي، د امنيتي ګواښونو نمونې وپېژني، او حتى د احتمالي خطرونو وړاندوينه وکړي. د بېلګې په توګه، د مصنوعي ځيرکتيا پر بنسټ سايبري دفاعي سيستمونه کولاى شي د شبکو غيرعادي فعاليتونه کشف کړي او د برېد له پېښېدو مخکې خبرداری ورکړي. دغه ډول سيستمونه په پرمختللو هېوادونو کې د ملي امنيت مهمه برخه ګرځېدلي دي (راسل او نورويګ، ۲۰۲۱).

سربېره پر دې، مصنوعي ځيرکتيا د استخباراتي تحليل په برخه کې هم ژور بدلون راوستى دى. پخوا به استخباراتي معلومات د انسانانو له خوا تحليل کېدل، چې وخت‌نيونکى او د تېروتنې احتمال پکې ډېر و. خو اوس د سيستمونه کولاى شي په څو ثانيو کې د ميليونونو معلوماتو تحليل وکړي، اړيکې وموميږي، او د تصميم نيونې لپاره دقيق معلومات وړاندې کړي. دا چاره د امنيتي ادارو د چټک او مؤثر غبرګون سبب ګرځي.

خو تخنيکي ظرفيت يوازې د پرمختللو وسايلو درلودلو معنا نه لري، بلکې د بشري منابعو کيفيت او مهارت هم پکې حياتي رول لري. يو هېواد که هر څومره پرمختللې ټکنالوژي ولري، خو که مسلکي، روزل شوي او متخصص کسان ونه لري، نو له دغې ټکنالوژۍ څخه به سمه ګټه وانخلي. له همدې امله، د بشري پانګې پراختيا د تخنيکي ظرفيت يوه مهمه برخه ده. دولتونه بايد په لوړو زده کړو، تخنيکي روزنو، او څېړنيزو پروګرامونو کې پانګونه وکړي، څو داسې متخصصين وروزي چې د مصنوعي ځيرکتيا سيستمونه طرحه، تحليل او کنټرول کړي.[1]

[1] Human Capital

په نړیواله کچه، پرمختللي هېوادونه لکه متحده ایالات او چین د مصنوعي ځیرکتیا په برخه کې د پراخو پانګونو له لارې خپل تخنیکي ظرفیتونه په بې‌ساري ډول لوړ کړي دي. دغه هېوادونه نه یوازې د د مصنوعي ځیرکتیا په اقتصادي ګټو تمرکز کوي، بلکې د ملي امنیت لپاره یې هم ستراتیژیک اهمیت ته پاملرنه کوي. د بېلګې په توګه، د ځارنې پرمختللي سیستمونه، د مخ پېژندنې ټکنالوژي، او خودکار دفاعي وسایل ټول د همدې پانګونو پایله ده (او ای سي ډي، ۲۰۱۹).[۱]

همدارنګه، تخنیکي ظرفیت د سایبري امنیت په برخه کې هم مهم رول لري. نن ورځ ډېرى امنیتي ګواښونه د انټرنېټ له لارې ترسره کېږي، لکه هکینګ، معلوماتي غلا، او د زیربناوو تخریب. هغه هېوادونه چې قوي سایبري دفاعي سیستمونه لري، کولی شي دغه ګواښونه په اغېزمن ډول مهار کړي. په مقابل کې، هغه هېوادونه چې په دې برخه کې کمزوري وي، د جدي امنیتي خطرونو سره مخ کېږي.

د تخنیکي ظرفیت بله مهمه برخه د نوښت او څېړنې وده ده.[۲] هغه هېوادونه چې د نوې ټکنالوژۍ د تولید وړتیا لري، نه یوازې مصرفوونکي پاتې کېږي، بلکې د ټکنالوژۍ تولیدوونکي ګرځي. دا چاره د اوږدمهاله امنیت او اقتصادي ثبات لپاره حیاتي ده. له همدې امله، د څېړنیزو مرکزونو، نوښتګر پروژو، او ټکنالوژیکو پارکونو جوړول د دولتونو لپاره یو مهم لومړیتوب ګڼل کېږي.

د افغانستان لپاره، د تخنیکي ظرفیت لوړونه باید له بنسټیزو پړاوونو څخه پیل شي. لومړی، د معلوماتي ټکنالوژۍ زده کړې ته باید جدي پاملرنه وشي، څو نوی نسل د ډیجیټلي نړۍ لپاره چمتو شي. دوهم، د سایبري امنیت په برخه کې د متخصصینو روزنه ضروري ده، ځکه چې افغانستان د سایبري ګواښونو پر وړاندې لا هم کمزورى دى. درېیم، د پوهنتونونو او تخنیکي انسټیټوټونو پیاوړتیا باید د دولت له لومړیتوبونو څخه وي، څو داخلي تخنیکي ظرفیت رامنځته شي.

سربېره پر دې، افغانستان کولی شي د نړیوالې همکارۍ له لارې خپل تخنیکي ظرفیت لوړ کړي. د روزنې پروګرامونه، تخنیکي مرستې، او د تجربو تبادله کولای شي د دې هېواد لپاره مهم فرصتونه برابر کړي. که افغانستان وکولی شي د ټکنالوژۍ په برخه کې بنسټیز پرمختګ وکړي، نو دا به د ملي امنیت په پیاوړتیا کې یو مهم ګام وي.

په پایله کې، تخنیکي ظرفیت د ملي امنیت یو اساسي رکن دى چې د مصنوعي ځیرکتیا په عصر کې یې اهمیت څو برابره شوى دى. هغه هېوادونه چې په دې برخه کې پانګونه کوي، نه یوازې د ګواښونو پر وړاندې مقاومت زیاتوي، بلکې د نړیوالو سیالیو په ډګر کې هم برلاسي ترلاسه کوي. د افغانستان لپاره، د تخنیکي ظرفیت لوړونه یو حیاتي ضرورت دى چې پرته له هغه د معاصر امنیتي ګواښونو پر وړاندې اغېزمن مقاومت ممکن نه دى.

دوهم بیان: د ټکنالوژۍ په برخه کې نړیواله همکاري

په معاصر نړیوال نظام کې امنیتي ګواښونه ورځ تر بلې نړیوال بُعد خپلوي، او نور د جغرافیایي پولو په چوکاټ کې نه محدودېږي. د مصنوعي ځیرکتیا چټک پرمختګ، سایبري جګړې، معلوماتي عملیات،

---

[۱] Organization for Economic Co-operation and Development
[۲] Innovation

او ډیجیټلي نفوذ داسې ماهیت لري چې کولی شي په ډېر لږ وخت کې له یوه هېواد څخه بل هېواد ته انتقال شي. له همدې امله، هېڅ هېواد نشي کولای یوازې د خپلو داخلي امکاناتو پر بنسټ د ټولو امنیتي ګواښونو مقابله وکړي. نړیواله همکاري د ملي امنیت د تأمین لپاره یو اساسي او نه جلا کېدونکی عنصر ګرځېدلی دی (ملګري ملتونه، ۲۰۲۰).

نړیواله همکاري په بېلابېلو برخو کې مهم رول لري. لومړی، د معلوماتو شریکول دي. کله چې یو هېواد د سایبري برید، ترهګریز فعالیت یا معلوماتي جګړې سره مخ کېږي، د نورو هېوادونو سره د استخباراتي او تخنیکي معلوماتو شریکول کولی شي د ګواښ سرچینه په چټکۍ سره وپېژني او د ورته بریدونو مخه ونیسي. دوهم، ګډ امنیتي عملیات دي، چې پکې هېوادونه په ګډه د سایبري جرمونو او نړیوالو ګواښونو پر وړاندې عملیات ترسره کوي. درېیم، تخنیکي ملاتړ او روزنه ده، چې له لارې یې پرمختللي هېوادونه خپل تخنیکي مهارتونه او تجربې له نورو هېوادونو سره شریکوي. څلورم، د نړیوالو معیارونو او اصولو جوړول دي، چې د مصنوعي ځیرکتیا او سایبري امنیت لپاره یو ګډ قانوني او اخلاقي چوکاټ رامنځته کوي.

په نړیوال ډګر کې بېلابېلې همکارۍ د دې اصل عملي بېلګې وړاندې کوي. د ایران او روسیې ترمنځ همکاري د سایبري او پوځي ټکنالوژۍ په برخه کې د پام وړ ده. دواړو هېوادونو په وروستیو کلونو کې د معلوماتي جګړې، ډرون ټکنالوژۍ، او سایبري وړتیاوو په برخه کې یو بل ته ملاتړ ورکړی دی. د بېلګې په توګه، د اوکراین په جګړه کې داسې راپورونه شته چې ایران د بې‌پیلوټه الوتکو په برخه کې له روسیې سره همکاري کړې، چې دا خپله د ټکنالوژیکي همکارۍ یوه ځرګنده نمونه ده. دغه ډول همکاري د دې لامل کېږي چې هېوادونه د لوړدیځو بندیزونو پر وړاندې بدیلې لارې وموميي او خپل امنیتي ظرفیتونه پیاوړي کړي.

له بلې خوا، د اوکراین او لوړدیځو هېوادونو ترمنځ همکاري د معاصر امنیتي همکارۍ یو پرمختللی مثال ګڼل کېږي. د روسیې له یرغل وروسته، لوړدیځو هېوادونو نه یوازې پوځي مرسته وکړه، بلکې د سایبري امنیت، استخباراتي معلوماتو شریکولو، او پرمختللو ټکنالوژیو په برخه کې یې هم پراخه همکاري وکړه. اوکراین د مصنوعي ځیرکتیا پر بنسټ د جګړې تحلیل، د سپوږمکۍ معلوماتو کارول، او د سایبري دفاع پرمختللي سیستمونه وکارول، چې دا ټول د نړیوالې همکارۍ پایله وه. دغه تجربه ښیي چې نړیواله همکاري کولی شي د یو هېواد د مقاومت او دفاع وړتیا څو برابره زیاته کړي. نړیوال سازمانونه هم په دې برخه کې مهم رول لري. د ملګرو ملتونو سازمان ، د اروپا اتحادیه ، او نور نړیوال بنسټونه د سایبري امنیت، مصنوعي ځیرکتیا، او نړیوالو ګواښونو د کنټرول لپاره اصول، پالیسۍ او چوکاټونه رامنځته کوي. دغه اصول د هېوادونو ترمنځ د باور فضا رامنځته کوي او د ګډو خطرونو پر وړاندې یو منظم دریځ تضمینوي. د نړیوالې همکارۍ بله مهمه ګټه د ټکنالوژۍ انتقال دی. پرمختللي هېوادونه کولی شي د روزنې، تجهیزاتو، تخنیکي مرستو او ګډو پروژو له لارې نورو هېوادونو ته خپل پرمختګ انتقال کړي. دا موضوع په ځانګړې توګه د هغو هېوادونو لپاره حیاتي ده چې لا هم د ټکنالوژۍ په لومړیو پړاوونو کې دي، ځکه چې دوی نشي کولای په یوازې ډول د پرمختللې ټکنالوژۍ لګښت او پوهه ترلاسه کړي.

د افغانستان لپاره نړیواله همکاري ځانګړی اهمیت لري. افغانستان د اوږدو جګړو، سیاسي بې‌ثباتۍ، او اقتصادي محدودیتونو له امله د پرمختللې ټکنالوژۍ په برخه کې له جدي ستونزو سره مخ دی. په ځانګړې توګه، له پاکستان سره وروستي سیاسي او امنیتي تنشونه دا څرګندوي چې افغانستان د سایبري او تخنیکي ظرفیت له اړخه کمزوری دی. که چېرې د معلوماتي جګړې، سایبري بریدونو یا ډیجیټلي نفوذ هڅې زیاتې شي، افغانستان به د دفاع لپاره کافي تخنیکي امکانات ونه لري. له همدې امله، افغانستان باید د نړیوالې همکارۍ له لارې خپل تخنیکي ظرفیت لوړ کړي، د سایبري امنیت بنسټونه پیاوړي کړي، او له نړیوالو تجربو څخه ګټه واخلي. دا همکاري کولی شي د روزنې پروګرامونه، تخنیکي مرستې، د معلوماتو شریکول، او د نړیوالو معیارونو پلي کول شامل کړي. سربېره پر دې، افغانستان باید هڅه وکړي چې په سیمه‌ییزه کچه هم همکاري پراخه کړي، څو د ګډو ګواښونو پر وړاندې یو منظم دریځ رامنځته شي. په پایله کې، نړیواله همکاري د معاصر امنیتي چاپېریال یو نه جلا کېدونکی عنصر دی. هغه هېوادونه چې له نورو سره همکاري کوي، نه یوازې خپل امنیتي ظرفیتونه پیاوړي کوي، بلکې د نړیوالو ګواښونو پر وړاندې اغېزمن او دوامداره مقاومت هم رامنځته کوي. په مقابل کې، هغه هېوادونه چې له نړیوالې همکارۍ څخه ځان لرې ساتي، د نوې ټکنالوژۍ له ګواښونو سره د مقابلې توان له لاسه ورکوي.

درېم بیان: نوې ټکنالوژي او د افغانستان ملي امنیت: د نړیوالې او سیمه‌ییزې همکارۍ ارزونه

افغانستان نه یوازې دا چې د نړیوالې همکارۍ او همغږۍ ته جدي اړتیا لري، بلکې د خپل جغرافیایي، سیاسي او امنیتي موقعیت له امله د سیمه‌ییزو رقابتونو او تاریخي کړکېچونو په منځ کې واقع شوی هېواد دی. په ځانګړې توګه، له پاکستان سره اوږدمهاله تاریخي تاوتریخوالی، د سرحدي شخړو دوام، او د متقابلو تورونو سیاست، د افغانستان امنیتي وضعیت لا پېچلی کړی دی. د امنیتي مطالعاتو له نظره، افغانستان د "امنیتي معما" یو روښانه مثال بلل کېدای شي. امنیتي معما هغه حالت ته ویل کېږي چې یو هېواد د خپل امنیت د زیاتولو لپاره اقدامات کوي، خو مقابل لوری دا اقدامات د ګواښ په توګه تعبیر کړي او په ځواب کې خپل پوځي او امنیتي ظرفیت لوړ کړي. دا حالت د باور فضا له منځه وړي او د تاوتریخوالي د زیاتېدو سبب ګرځي. د افغانستان او پاکستان ترمنځ اړیکې تر ډېره حده د همدې معما تر اغېز لاندې دي، چې دواړه لوري د یو بل اقدامات د ګواښ په توګه ګڼي.[1]

په معاصر وخت کې، دا امنیتي سیالي یوازې په دودیزو وسلو محدوده نه ده پاتې شوې، بلکې نوې ټکنالوژۍ لکه بې‌پیلوټه الوتکې (ډرون)، جنګي جېټ الوتکې، سایبري وسایل، او استخباراتي سیستمونه پکې مهم رول لري. پاکستان د پوځي ټکنالوژۍ په برخه کې نسبي پرمختګ کړی، په ځانګړې توګه د ډرون کارونې، ځارنې سیستمونو، او استخباراتي شبکو په برخه کې. په مقابل کې، افغانستان د دغو پرمختللو ټکنالوژیو له اړخه محدود ظرفیت لري، چې دا وضعیت د ځواک د توازن په برخه کې یو ډول نابرابري رامنځته کوي.

[1] Security Dilemma: A situation where a state's efforts to increase its security unintentionally make other states feel less secure, leading to tension and rivalry.

بې‌پیلوټه الوتکې (ډرونونه) د معاصر امنیت یوه مهمه وسیله ګرځېدلې ده. دغه وسایل کولی شي د ځارنې، هدف ټاکلو، او حتی بریدونو لپاره وکارول شي. هغه هېوادونه چې پرمختللي ډرون سیستمونه لري، کولی شي له لرې واټن څخه دقیق عملیات ترسره کړي. افغانستان چې په دې برخه کې محدود امکانات لري، نه یوازې د دفاع په برخه کې له ستونزو سره مخ دی، بلکې د ځارنې او استخباراتي معلوماتو په راټولولو کې هم له کمزورتیاوو سره مخامخ دی. همدارنګه، جنګي جېټ الوتکې او پرمختللي هوایي سیستمونه د امنیتي توازن په ټاکلو کې مهم رول لري. که یو هېواد پرمختللی هوایي ځواک ولري، کولی شي په لنډ وخت کې د مقابل لوري پر اهدافو اغېز وکړي. افغانستان په دې برخه کې هم له تخنیکي، مالي او لوژستیکي ستونزو سره مخ دی، چې دا د هوایي دفاع او برید وړتیاوې محدودوي. د استخباراتي سیستمونو په برخه کې هم ورته وضعیت لیدل کېږي. پرمختللي هېوادونه د مصنوعي ځیرکتیا پر بنسټ استخباراتي تحلیلونه، د معلوماتو لوی بانکونه (لویه ډیټا)، او پرمختللي ځارنیز سیستمونه کاروي. په مقابل کې، افغانستان لا هم د دودیزو استخباراتي میتودونو پر بنسټ ولاړ دی، چې دا کار د معلوماتو د دقیق تحلیل او پر وخت پرېکړې نیولو وړتیا کموي.

د دې ټولو ستونزو تر څنګ، سایبري امنیت هم یوه مهمه برخه ده. افغانستان د سایبري دفاع په برخه کې محدود ظرفیت لري، چې دا کولای شي د معلوماتي جګړې، جعلي خبرونو، او سایبري بریدونو پر وړاندې هېواد زیانمن کړي. په ځانګړې توګه، د ټولنیزو رسنیو له لارې د عامه افکارو اغېزمنول کولای شي سیاسي او ټولنیز ثبات ته زیان ورسوي. په همدې اساس، نړیواله همکاري د افغانستان لپاره یوازې یو انتخاب نه، بلکې یوه اړتیا ده. افغانستان کولی شي د نړیوالو شریکانو سره د همکارۍ له لارې خپل تخنیکي ظرفیت لوړ کړي، د ډرون او سایبري ټکنالوژۍ په برخه کې پرمختګ وکړي، استخباراتي سیستمونه عصري کړي، او د نړیوالو تجربو څخه ګټه واخلي. دا همکاري باید د روزنې، تجهیزاتو، معلوماتو شریکولو، او ګډو امنیتي پروګرامونو په بڼه وي.

سربېره پر دې، افغانستان باید هڅه وکړي چې د سیمه‌ییزې همکارۍ له لارې د باور فضا رامنځته کړي. که څه هم له پاکستان سره سیاسي ستونزې شته، خو د اوږدمهاله امنیت لپاره اړینه ده چې د خبرو، همغږۍ او اعتماد جوړونې میکانیزمونه رامنځته شي، څو د امنیتي معما شدت کم شي. د افغانستان امنیتي وضعیت د نوې ټکنالوژۍ، سیمه‌ییزو رقابتونو، او داخلي محدودیتونو تر اغېز لاندې دی. نړیواله همکاري کولی شي د دې ستونزو د حل لپاره یوه مهمه وسیله وګرځي. که افغانستان وکولی شي له نړیوالو فرصتونو څخه ګټه واخلي او خپل تخنیکي او امنیتي ظرفیتونه لوړ کړي، نو کولای شي د معاصر امنیتي ګواښونو پر وړاندې یو قوي او دوامداره دریځ خپل کړي.

څلورم بیان: د ګواښونو مدیریت لپاره ستراتیژي

د ګواښونو اغېزمن مدیریت ډېر مهم دی، ځکه چې دا د احتمالي زیانونو مخه نیسي او د اداري اوږدمهاله ثبات تضمینوي. د دې لپاره یوه بنسټیزه تګلاره د خطر پېژندنه او ارزونه ده. په دې بهیر کې خطرونه په منظم ډول پېژندل کېږي او ارزول کېږي چې کوم خطرونه پر اداره اغېز کولای شي. دا کار عموماً د داسې وسیلو له لارې ترسره کېږي لکه د قوتونو، کمزوریو، فرصتونو او ګواښونو (سوات) تحلیل او د خطر نقشه

جوړونه. کله چې خطرونه پر وخت وپېژندل شي، اداره کولای شي هغوی د احتمال او اغېز له مخې درجه‌بندي کړي او بیا ورته مناسب اقدامات طرحه کړي.[۱] بله مهمه تګلاره د خطر کمول دي. دا مانا لري چې هغه خطرونه چې پېژندل شوي، د هغوی اغېز راکم شي یا مخه یې ونیول شي. دا کار په ښلابښلو لارو ترسره کېدای شي، لکه د کنټرولي تدابیرو جوړول، پانګونه په ښلابښلو برخو وېشل، او یا نوې ټکنالوژي کارول. د ښلګې په توګه، که پانګونه په مختلفو برخو کې ووېشل شي، نو د بازار د بدلون خطر کمېږي. همدارنګه، د خوندیتوب قوي اصول او د بیړنیو حالاتو پلانونه د عملي ګډوډۍ خطر راکموي. د خطر کمول یو دوامداره بهیر دی او باید تل وڅارل شي او د حالاتو له بدلون سره سم اصلاح شي.[۲] د خطر د مدیریت بله مهمه برخه د خطر انتقال دی. په دې کې اداره هڅه کوي چې د خطر مسؤلیت بل لوري ته وسپاري. دا کار د بیمې، د کارونو د سپارلو (بهرنۍ همکارۍ)، او یا قراردادونو له لارې ترسره کېږي. د ښلګې په توګه، یو شرکت کولای شي بیمه واخلي څو که مالي زیان پېښ شي، تاوان یې جبران شي. همدارنګه، ځینې چارې متخصصو ادارو ته سپارل د عملي خطرونو کچه راکموي. دا چاره ادارو ته دا فرصت برابروي چې پر خپلو اصلي فعالیتونو تمرکز وکړي.د خطر په مدیریت کې اړیکه او د اړخونو ګډون هم ډېر مهم دي. شفافه اړیکه له کارکوونکو، پانګه‌والو او مشتریانو سره دا یقیني کوي چې ټول د خطرونو او د حل لارو په اړه خبر وي. د اړخونو ګډون باور زیاتوي او همکاري پیاوړې کوي. منظم راپورونه، روښانه معلومات او د نظر اخیستنې سیستمونه د اغېزمن خطر مدیریت مهم عناصر دي. دا کار ادارو سره مرسته کوي چې نامعلومو حالاتو ته مناسب ځواب ووایي او خپلې تګلارې د خلکو له تمو سره برابرې کړي (خان، ۲۰۲۴: ۱۱۶–۱۱۷). د ګواښونو مدیریت لپاره ستراتیژي د مصنوعي ځیرکتیا د خوندي او اغېزمنې کارونې لپاره یو مهم اصل ګڼل کېږي. ځکه چې د مصنوعي ځیرکتیا سیستمونه له ښلابښلو احتمالي خطرونو سره مخ کېدای شي، نو د خطرونو پېژندنه، ارزونه او د هغوی د اغېزو کمول د دې ټکنالوژۍ د بریالي مدیریت لپاره اړین دي. د خطرونو منظم تحلیل، لکه د قوتونو، کمزوریو، فرصتونو او ګواښونو (سوات) ارزونه، مرسته کوي چې احتمالي ستونزې له مخکې وپېژندل شي او د مخنیوي لپاره ورته مناسبې لارې چارې جوړې شي. همدارنګه، د خطرونو کمول د دې سبب کېږي چې د مصنوعي ځیرکتیا سیستمونه په خوندي او دوامداره ډول فعالیت وکړي. د کنټرولي تدابیرو جوړول، د امنیتي اصولو پیاوړتیا او د بیړنیو حالاتو لپاره د پلانونو رامنځته کول هغه لارې دي چې د احتمالي زیانونو کچه راکموي. سربېره پر دې، د خطر انتقال او له متخصصو ادارو سره همکاري کولای شي د مدیریت وړتیا لوړه کړي او د ادارو لپاره د ستونزو د حل زمینه برابره کړي.

په ټوله کې، د مصنوعي ځیرکتیا د ګواښونو مدیریت یوازې تخنیکي اقدام نه دی، بلکې د منظم پلان جوړونې، شفافې اړیکې او د ټولو اړخونو د ګډون اړتیا لري. کله چې اداري د خطرونو د پېژندنې، ارزونې

[۱] SWOT Analysis

[۲] Risk Management, Risk Identification, Risk Assessment,Risk Mapping, Risk Mitigation, Risk Transfer, Insurance, Outsourcing, Stakeholder Engagement

او کنټرول لپاره واضح ستراتيژي ولري، نو کولای شي مصنوعي ځيرکتيا په داسې ډول وکاروي چې هم امنيتي خطرونه کم شي او هم د دې ټکنالوژۍ ګټې په اغېزمنه توګه ترلاسه شي.

مناقشه

د نویو ټکنالوژیو، په ځانګړي ډول د مصنوعي ځیرکتیا، اغیز پر ملي امنیت یوه پیچلې او څو اړخیزه موضوع ده چې د معاصر نړیوال نظام په کچه یې د دولتونو د امنیتي لیدلورو بڼه بدله کړې ده. د دې څېړنې د موندنو له مخې، مصنوعي ځیرکتیا نه یوازې د امنیت د پیاوړتیا لپاره یو مهم فرصت دی، بلکې په ورته وخت کې نوي ګواښونه او ننګونې هم رامنځته کوي. له همدې امله، د مصنوعي ځیرکتیا اغیز باید یوازې د مثبت یا منفي اړخ له مخې ونه ارزول شي، بلکې د دولتونو د مدیریت، پالیسۍ او د کارونې د طریقې پر بنسټ باید تحلیل شي.

د څېړنې له تحلیل څخه څرګندېږي چې مصنوعي ځیرکتیا د ملي امنیت په بېلابېلو برخو کې د دولتونو وړتیاوې زیاتولی شي. د استخباراتي معلوماتو د چټک تحلیل، د امنیتي ګواښونو د وړاندوینې، د سایبري دفاع د پیاوړتیا او د پوځي سیستمونو د پرمختګ په برخه کې مصنوعي ځیرکتیا د دولتونو لپاره نوي امکانات رامنځته کړي دي. هغه دولتونه چې د دې ټکنالوژۍ د پراختیا، څېړنې او کارونې لپاره لازم ظرفیتونه لري، کولای شي د امنیتي پرېکړو په برخه کې له نورو دولتونو څخه نسبي برلاسي ترلاسه کړي. له بلې خوا، د مصنوعي ځیرکتیا پراختیا د ملي او نړیوال امنیت لپاره ځینې جدي ننګونې هم رامنځته کوي. د سایبري بریدونو د پېچلتیا زیاتوالی، د معلوماتو د ناسمې کارونې امکان، د جعلي معلوماتو خپرېدل، د شخصي حریم ګواښ او د خپلواکو وسلو د پراختیا موضوع هغه مسایل دي چې د دولتونو پاملرنې ته اړتیا لري. که د مصنوعي ځیرکتیا کارونه له قانوني، اخلاقي او امنیتي چوکاټونو پرته ترسره شي، نو دا ټکنالوژي کولای شي د امنیت د پیاوړتیا پر ځای د بې‌ثباتۍ سبب وګرځي.

د نړیوالو اړیکو د نظریو له لیدلوري هم د مصنوعي ځیرکتیا اغیز بېلابېل تعبیرونه لري. ریالیستان ټکنالوژیکي وړتیا د دولتونو د ځواک او سیالۍ له مهمو عناصرو څخه ګڼي او باور لري چې پرمختللې ټکنالوژي کولای شي د نړیوال ځواک توازن بدل کړي. په مقابل کې، لیبرال نظریه‌پوهان ټینګار کوي چې نړیواله همکاري، ګډ قوانین او علمي تبادله کولای شي د مصنوعي ځیرکتیا له خطرونو څخه د مخنیوي لپاره اغیزمن رول ولري. همدارنګه، سازه‌انګاران بیا د دې موضوع پر ټولنیزو ارزښتونو، اخلاقي معیارونو او د امنیت د مفهوم پر بدلېدونکي ماهیت تمرکز کوي. د دې څېړنې له مخې، د مصنوعي ځیرکتیا د اغیزمنې کارونې لپاره یوازې د ټکنالوژۍ درلودل کافي نه دي، بلکې دولتونه باید د پالیسۍ جوړونې، قانوني تنظیم، بشري ظرفیت جوړونې او نړیوالې همکارۍ په برخو کې هم لازم اقدامات ترسره کړي. هغه دولتونه چې د مصنوعي ځیرکتیا د کارونې لپاره روښانه ستراتیژي ولري، کولای شي له دې ټکنالوژۍ څخه د ملي امنیت د پیاوړتیا لپاره ګټه واخلي او احتمالي ګواښونه یې محدود کړي. په پایله کې، ویلای شو چې مصنوعي ځیرکتیا د ملي امنیت په ډګر کې دوه ګونی رول لري؛ له یوې خوا د امنیتي وړتیاوو د لوړولو، د ګواښونو د مخنیوي او د پرېکړه‌نیونې د ښه والي وسیله ده، او له بلې خوا د نویو امنیتي ننګونو سرچینه کېدای شي. نو د دې ټکنالوژۍ راتلونکی اغیز تر ډېره د دولتونو د مدیریت، مسؤلانه کارونې او د مناسبو امنیتي تګلارو له شتون سره تړاو لري.

پایلـه

لکه څنګه چې په دې څېړنه کې په تفصیل سره وڅېړل شول، نوې ټکنالوژۍ په ځانګړې توګه مصنوعي ځیرکتیا د معاصر نړیوال نظام په امنیتي، سیاسي او پوځي جوړښت کې بنسټیز بدلونونه رامنځته کړي دي. نن ورځ ټکنالوژي یوازې یو مرستندویه وسیله نه ده، بلکې د دولتونو د قدرت، نفوذ او ملي امنیت یو اساسي ټاکونکی عنصر ګرځېدلی دی.

د مصنوعي ځیرکتیا پرمختګ د دې لامل شوی چې د جګړې او امنیت بڼه له دودیز حالت څخه واوړي او نوې بڼه غوره کړي. په ځانګړې توګه، خپلواک وسایل لکه بې‌پیلوټه الوتکې (ډرونونه)، هوښیار توغندي، او اتومات دفاعي سیستمونه د جګړې ماهیت بدل کړی دی. ډرون الوتکې کولی شي پرته له مستقیم انساني مداخلې څخه هدفونه وڅاري، تحلیل کړي او حتی برید پرې ترسره کړي. دا ډول ټکنالوژي د جګړې لګښت کموي، خو په عین وخت کې د اخلاقي، حقوقي او امنیتي ستونزو سبب هم ګرځي. هغه هېوادونه چې پرمختللي ډرون او مصنوعي ځیرکتیایي سیستمونه لري، کولی شي په لرې واټن کې دقیق او چټک عملیات ترسره کړي، چې دا د قدرت په توازن کې لوی بدلون رامنځته کوي.

له بلې خوا، سایبري جګړه د ملي امنیت یو له مهمو ننګونو څخه ګرځېدلې ده. سایبري بریدونه، هک کول، د معلوماتو غلا، او د حیاتي زیربناوو ګډوډول هغه ګواښونه دي چې کولی شي د یو هېواد اقتصادي، سیاسي او امنیتي ثبات له خطر سره مخ کړي. د بېلګې په توګه، که د یو هېواد د برېښنا سیستم، بانکداري شبکه، یا مخابراتي سیستم هک شي، نو دا کولای شي ټول هېواد فلج کړي. مصنوعي ځیرکتیا په دې برخه کې دواړه رولونه لري: هم د برید وسیله ګرځي او هم د دفاع لپاره کارېدلی شي.

سربېره پر دې، معلوماتي جګړه هم د مصنوعي ځیرکتیا له امله لا پېچلې شوې ده. ژور جعل کاري مواد (ډیپ فیک)، جعلي خبرونه، او هدفمند تبلیغات کولی شي عامه افکار منحرف کړي، سیاسي بې‌ثباتي رامنځته کړي، او حتی د دولتونو مشروعیت تر پوښتنې لاندې راولي. دا ډول ګواښونه په ځانګړې توګه د هغو هېوادونو لپاره خطرناک دي چې د معلوماتي کنټرول او عامه پوهاوي سیستمونه کمزوري لري.

په دې اساس، نوې ټکنالوژي دوه اړخیزه ماهیت لري: له یوې خوا د ځواک او امنیت د زیاتوالي وسیله ده، او له بلې خوا د نوو ګواښونو سرچینه. نو ځکه، ټکنالوژي په ذات کې نه منفي ده او نه مثبته، بلکې د هغې اغېز د کارونې له څرنګوالي سره تړاو لري. د معاصر نړیوال وضعیت په نظر کې نیولو سره، هېوادونه اړ دي چې د خپل ملي امنیت د پیاوړتیا لپاره څو اساسي ګامونه پورته کړي: لومړی، باید خپل تخنیکي ظرفیت لوړ کړي، په ځانګړې توګه د مصنوعي ځیرکتیا، سایبري امنیت او دفاعي ټکنالوژۍ په برخه کې پانګونه وکړي. دوهم، باید د سایبري دفاع قوي سیستمونه رامنځته کړي تر څو د هک او سایبري بریدونو پر وړاندې مقاومت ولري. دریم، باید د مصنوعي ځیرکتیا د کارونې لپاره واضح قانوني او اخلاقي چوکاټ جوړ کړي، څو د ناوړه استفادې مخه ونیول شي. څلورم، نړیواله او سیمه‌ییزه همکاري پیاوړې کړي، ځکه چې معاصر ګواښونه یوازې د یو هېواد په کچه نشي مهار کېدای. پنځم، باید د عامه پوهاوي کچه لوړه کړي تر څو خلک د معلوماتي جګړې او جعلي خبرونو پر وړاندې هوښیار شي. په ځانګړې توګه د

افغانستان لپاره، دا موضوع لا ډېره حياتي ده. افغانستان چې د ټکنالوژۍ له اړخه محدود ظرفيت لري، بايد د نړيوالې همکارۍ له لارې خپل سايبري، استخباراتي او تخنيکي سيستمونه پياوړي کړي. که دا کار ترسره نه شي، نو هېواد به د سايبري بريدونو، معلوماتي جګړې او تخنيکي برلاسۍ لرونکو هېوادونو پر وړاندې زيانمن پاتې شي. په پای کې، دا ويلای شو چې په معاصر نړيوال نظام کې د ملي امنيت بنسټونه د ټکنالوژۍ سره ژور تړاو لري. هغه هېوادونه به بريالي وي چې وکولی شي د نوې ټکنالوژۍ فرصتونه په سمه توګه وکاروي، ګواښونه يې مديريت کړي، او خپل امنيتي ستراتيژي د ټکنالوژۍ له پرمختګ سره عيار کړي. برعکس، هغه هېوادونه چې له دې بدلونونو سره ځان عيار نه کړي، د امنيتي کمزورتيا او نړيوالې سيالۍ خخه د پاتې کېدو له جدي خطر سره مخ کېږي.

وړاندیزونه

د دې څېړنې د موندنو او تحلیلونو پر بنسټ، لاندې وړاندیزونه وړاندې کېږي:

۱. د مصنوعي ځیرکتیا لپاره د ملي تګلارې جوړول: دولتونه باید د مصنوعي ځیرکتیا د پراختیا او کارونې لپاره روښانه ملي تګلاره جوړه کړي، څو د دې ټکنالوژۍ له فرصتونو څخه په اغېزمن ډول ګټه واخیستل شي او احتمالي امنیتي ګواښونه یې مدیریت شي.

۲. د تخنیکي او بشري ظرفیتونو پیاوړتیا: د مصنوعي ځیرکتیا اغېزمنه کارونه د مسلکي کادرونو، څېړونکو او تخنیکي متخصصینو شتون ته اړتیا لري. له همدې امله دولتونه باید د زده‌کړې، څېړنې او روزنې په برخو کې پانګونه زیاته کړي.

۳. د سایبري امنیت پیاوړتیا:د مصنوعي ځیرکتیا د پراختیا ترڅنګ باید د سایبري امنیت سیستمونه هم پیاوړي شي، ځکه چې د دې ټکنالوژۍ ناوړه استفاده کولای شي د دولتونو مهم معلومات او امنیتي جوړښتونه له ګواښ سره مخ کړي.

۴. د مصنوعي ځیرکتیا د کارونې لپاره قانوني او اخلاقي چوکاټ رامنځته کول:

دولتونه باید داسې قوانین او مقررات جوړ کړي چې د مصنوعي ځیرکتیا کارونه د بشري حقونو، شخصي محرمیت او نړیوالو اصولو له معیارونو سره برابر کړي.

۵. په امنیتي او دفاعي برخو کې د مسؤلانه کارونې تګلاره: مصنوعي ځیرکتیا باید د دفاعي او امنیتي موخو لپاره په داسې ډول وکارول شي چې د انساني څارنې اصل پکې خوندي وي او د هغې ناوړه کارونه د جګړو او بې‌ثباتۍ سبب نه شي.

٦. د معلوماتو د خوندیتوب او مدیریت پیاوړتیا: څرنګه چې مصنوعي ځیرکتیا د لویو معلوماتو پر تحلیل ولاړه ده، نو دولتونه باید د معلوماتو د راټولولو، ساتنې او کارونې لپاره خوندي سیستمونه رامنځته کړي.

۷. د نړیوالې همکارۍ پراختیا: د مصنوعي ځیرکتیا ګواښونه یوازې د یوه هېواد په کچه نه محدودېږي؛ له همدې امله دولتونه باید د نړیوالو سازمانونو او نورو هېوادونو سره د تجربو، معلوماتو او تخنیکي وړتیاوو د شریکولو لپاره همکاري زیاته کړي.

۸. د څېړنې او نوښت ملاتړ: دولتونه باید د پوهنتونونو، څېړنیزو مرکزونو او خصوصي سکټور ترمنځ همغږي رامنځته کړي، څو د مصنوعي ځیرکتیا په برخه کې علمي څېړنې او نوښتونه وده وکړي.

۹. د مصنوعي ځیرکتیا د احتمالي ګواښونو لپاره د چمتووالي پلان جوړول:

امنیتي ادارې باید د مصنوعي ځیرکتیا له امله رامنځته کېدونکو احتمالي ګواښونو، لکه سایبري بریدونو، معلوماتي جګړو او د جعلي معلوماتو خپرېدو لپاره ځانګړي پلانونه ولري.

۱۰. د ټکنالوژۍ او ملي امنیت ترمنځ د متوازن چلند رامنځته کول:

دولتونه باید مصنوعي ځیرکتیا نه یوازې د امنیتي ګواښ په توګه او نه یوازې د فرصت په توګه وګوري، بلکې دې ټکنالوژۍ د ګټو او خطرونو ترمنځ متوازن دریځ غوره کړي.

اخځليکونه

احمدي، علي، افشين زرگر، او آدمی. ۱۴۰۲. «*فناوري هوش مصنوعي و تغيير در امنيت ملي دولت‌ها*». فصلنامه سياست دفاعي، ۳۳ (۱۲۳):ص ۱۲۳–۱۴۶.
لينک: https://www.sid.ir

احمدي، علي، افشين زرگر، او آدمی. ۱۴۰۱. «*نقش فناوری‌های نوظهور در امنيت و قدرت ملي کشورها: فرصت‌ها و تهديدها*». فصلنامه مطالعات بين‌المللي، ۱۸ (۴):ص ۱۳۹–۱۵۹.
لينک: https://doi.org/۱۰,۲۲۰۳٤/ISJ.۲۰۲۱,۲۷۹۸٤۰,۱٤۲

روزنا، جيمز، او نور. انقلاب *اطلاعات، امنيت و فناوری‌های جديد*. *ژباړن: عليرضا طيب*. تهران: پژوهشکده مطالعات راهبردي. ۱۳۹۰.

روشندل، جليل. امنيت ملی و نظام بين‌المللی. چاپ نهم. تهران: سازمان مطالعه و تدوين کتب علوم انسانی پوهنتون (سمت). ۱۳۹۳.

سجادي، سيد عبدالقيوم. ۱۴۰۴. «*هوش مصنوعي و تحول ماهيت امنيت بين‌الملل*». مطالعات سياسی و بين‌المللی. کابل: پوهنتون خاتم‌النبيين، ۲ (۵): ۲۵–۴۸.

سيف‌زاده، سيدحسين. ۱۳۸۵. معمای امنيت و چالش‌های جديد غرب. تهران: دفتر مطالعات سياسی و بين‌المللی.

نجيب محمود، سيد احمد. امنيت بين‌الملل. کابل: کابل پوهنتون، انتشارات او فوتوکاپي سيدحسيب‌الله. ۱۴۰۴.

نظري، علي اشرف. ۱۴۰۳. «*هوش مصنوعي و تحول بنيادين در سياست‌گذاری‌های امنيتي–دفاعي: درک جايگاه امنيت انساني*». فصلنامه سياست‌گذاری عمومي، ۱۰ (۱):ص ۵۴–۷۴.
لينک: https://doi.org/۱۰,۲۲۰۵۹/jpolicy.۲۰۲٤,۹۹۸۲٦

نورمحمدي، مرتضی، او مجتبی تقی‌پور. ۱۴۰۴. «*تأثير هوش مصنوعي بر ماهيت جنگ‌ها*». فصلنامه مطالعات سياسی و راهبردي جمهوری اسلامي ايران، ۹ (۳۰).

مبين، تاج محمد. ۱۴۰۲. مصنوعي ځيرکتيا. کندهار: کندهار پوهنتون، ډيجيټل کتابتون. د لاسرسي وړ: https://ketabton.com

ميکائيل، پژمان المام طالش، کريمي، او اوروجي. ۱۴۰۳. «توسل دولت‌ها به هوش مصنوعي جهت تأمين امنيت ملی و مواجهه با تهديدات حقوق بشري». دولت‌پژوهی ايران معاصر، ۱۰ (۱): ۳۹–۶۵.

منفرد، حسن محمد، او تيرزاد تقی‌پور جاوي. ۱۴۰۳. «نقش فناوری هوش مصنوعي در دگرگوني ماهيت جنگ: براساس مطالعه اسناد راهبردي رژيم صهيونيستي». مطالعات بنيادين و کاربردي جهان اسلام، ٦ (۲۲): ۲۸۵–۳۰٦.
لينک: https://doi.org/۱۰,۲۲۰۳٤/fasiw.۲۰۲۵,٤۸۳٦۵۹,۱۳۹٤

حسيني، سيد اميرحسين، او عليرضا هاشمي‌زاده. ۱۴۰۳. «هوش مصنوعي و صلح و امنيت بين‌المللي». فصلنامه پژوهش‌های روابط بين‌الملل، ۱۵ (۲): ۲۲۵–۲۴۵.

فيروزآبادي، سيد جلال دهقاني، او سعيد جهان‌آزاد. ۱۴۰۲. «هوش مصنوعي و مسئله‌دار کردن درون‌مايه‌های امنيت ملي». فصلنامه علمی پژوهش‌های راهبردي سياست، ۱۲ (۴۶): ۲۰۹–۲۲۴.

لينک: https://doi.org/۱۰,۲۲۰۵٤/QPSS.۲۰۲۲,۷۰٦۹۰,۳۱۳۰

English Sources and References

Ahmadi, A., Zargar, A., & Adami, A. 2022. "The Role of Emerging Technologies in National Security and Power of Countries: Opportunities and Threats." International Studies Journal (ISJ), 18(4): 139–159. https://doi.org/10.22034/ISJ.2021.279840.1427

Allen, G., & Chan, T. 2017. Artificial Intelligence and National Security. Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/publication/artificial-intelligence-and-national-security

Buchanan, B. 2020. The AI Triad and What It Means for National Security Strategy. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/the-ai-triad-and-what-it-means-for-national-security-strategy

Congressional Research Service. 2018. Artificial Intelligence and National Security (Report No. R45178). https://crsreports.congress.gov

Khan, A. 2024. "Artificial Intelligence in National Security: Opportunities and Risks." Farl Journal of Global Affairs and Security Studies, 1(2). https://doi.org/10.47305/FJGASS.2024.1.45

Ortega, A. 2025. AI Threats to National Security Can Be Countered Through an Incident Regime. https://arxiv.org/abs/2503.19887

Rai, D. H. 2024. Artificial Intelligence Through Time: A Comprehensive Historical Review. Unpublished manuscript or preprint.

Russell, S. J., & Norvig, P. 2010. Artificial Intelligence: A Modern Approach. 3rd ed. Prentice Hall.

Sarwar, G., & Rashid, M. I. 2025. "Artificial Intelligence in Pakistan's National Security Strategy: Evolution and Impacts." Journal of Applied Linguistics and TESOL (JALT), 8(2): 1338–135X.

Spahr, T. W. 2024. "Raven Sentry: Employing AI for Indications and Warnings in Afghanistan." Parameters, 54(2). https://doi.org/10.55540/0031-1723.328