DEFENSE RESEARCH INSTITUTE OF MONGOLIA

Journal of Security and Defense Studies

Journal homepage:
https://mids.gov.mn/category/ayulgui_baidal-2/

ISSN: 2220-9115, E-ISSN: 2708-1230

Research Article

DOI: https://doi.org/10.65816/jsds.2026.02.011

Cyberspace and the Transformation of the Defense Sector

Dorjpalam Khulan

Lieutenant, Master's degree, Instructor, Department of Cyber Security, National Defense University of Mongolia, E-mail address: khulandorjpalam@gmail.com

Received: 16 June 2026 *Revised: 26 June 2026*
Accepted: 28 June 2026 *Published online: 28 July 2026*

ABSTRACT

This article examines cyberspace as a strategic military domain and analyzes the institutional, training, and human resource transformations required for armed forces to operate effectively in cyber-enabled conflicts. The study employs theoretical and comparative analysis by reviewing policy documents, organizational reforms, and training approaches across NATO and selected national cases (United States, Germany, United Kingdom, Russia, China, and Estonia). The findings indicate that cyber capability development cannot be reduced to technical modernization alone; rather, it depends on a coherent triad of reforms: (i) a clear command-and-control model with defined authorities and rapid decision cycles; (ii) practice-oriented training built on simulation, red/blue teaming, and command-staff exercises; and (iii) an adaptive human resource policy that enables recruitment, retention, and continuous professional development. The article argues that treating cyberspace as a standalone domain reshapes doctrine, force design, and training outcomes, and it provides a structured pathway for capability maturation through phased institutional and training development.

Keywords: *cybersecurity; cyberspace; cyber domain; military training; cyber command; red team/blue team; continuous capability development; human resource policy*

Кибер орон зай ба батлан хамгаалах салбарын өөрчлөлт

Доржпалам Хулан

Үндэсний батлан хамгаалахын их сургуулийн Цэргийн нэгдсэн сургуулийн Кибер аюулгүй байдлын тэнхимийн багш, магистр, дэслэгч, khulandorjpalam@gmail.com

ХУРААНГУЙ

Энэхүү өгүүлэл нь кибер орон зайг мэдээллийн технологийн дэд бүтцийн харилцан хамааралтай сүлжээнүүдээс бүрдэх шинэ стратегийн талбар хэмээн авч үзэж, зэвсэгт хүчний удирдлага, сургалт болон хүний нөөцийн бодлогод гарч буй өөрчлөлтүүдийг судалсан болно. Судалгаанд онолын дүн шинжилгээ, олон улсын туршлага, харьцуулсан судалгааны аргыг ашиглаж, НАТО, АНУ, Герман, Их Британи, ОХУ, БНХАУ, Эстони зэрэг улсын туршлагыг авч үзлээ. Кибер орон зайг тав дахь мөргөлдөөний домэйн гэж үзэх онолын байр суурь, кибер хүчний бүтэц,

удирдлагын шинэчлэл, red/blue team сургалт болон тасралтгүй чадавхжуулалтын чиг хандлага зэрэг асуудлыг хамарсан болно. Судалгааны үр дүнд кибер орон зай нь зөвхөн техникийн асуудал бус, стратеги, байгууллага, хүний хүчин зүйлийг цогцоор нь шинэчлэх шаардлагатайг тодорхойлсон. Энэ нь батлан хамгаалах салбарт хүний нөөцийн бодлого, удирдлагын бүтэц, сургалтын тогтолцоог нэгдсэн стратегийн хүрээнд хөгжүүлэх зайлшгүй шаардлагатайг нотолж байна.

Түлхүүр үгс: *кибер аюулгүй байдал, кибер орон зай, кибер дайн, кибер цэрэг, цэргийн удирдлага, сургалтын чиг хандлага, кибер командлал.*

ОРШИЛ

Орчин үеийн цэргийн ажиллагааны хэлбэр, цар хүрээ улам нарийссантай холбоотойгоор зэвсэгт хүчнийг мэргэжлийн түвшинд хөгжүүлэх нь үндэсний аюулгүй байдал, олон улсын тогтвортой байдлыг хангах стратегийн үндсэн нөхцөл болж байна. Үүнтэй зэрэгцэн кибер орон зай нь газрын, тэнгисийн, агаарын болон сансрын орон зайг дагасан уламжлалт талбаруудын дараах тав дахь мөргөлдөөний талбар төдийгүй, тайван цаг, дайн бүхий байдал, дайны байдалд гэсэн бүх үе шатанд тасралтгүй үргэлжилдэг стратегийн орчин болон төлөвшиж байна.

Кибер орон зай нь өгөгдөл дамжих хурд, өгөгдөлд суурилсан шийдвэр гаргалт, сүлжээний хамгаалалтаар дамжин батлан хамгаалах чадавх, стратегийн тэнцвэрт байдалд шууд нөлөөлж байна. Үүнийг АНУ-ын зэвсэгт хүчний кибер бодлого, төсвийн өөрчлөлтийг шинжилсэн судалгаанд мэдээлэл, харилцаа холбооны технологийг орчин үеийн цэргийн байгууллагын “холбогч эд” хэмээн тодорхойлсон нь баталж байна. Иймээс орчин үеийн зөрчил, сөргөлдөөн нь уламжлалт зэвсгийн хэрэглээнээс гадна “бит ба байтын түвшинд” өрнөх шинэ хэлбэрт шилжиж байна.

Гэвч “кибер орон зай”-г стратегийн талбар болгон тодорхойлох нэр томьёо, ойлголт нь өнөө хэр нэгдмэл бус хэвээр байна. “Кибер” гэх ойлголтыг зарим нь компьютер, сүлжээ, мэдээллийн баталгаат байдлын хүрээнд тайлбарладаг бол, нөгөө хэсэг нь цахим орон зай дахь бүх төрлийн мэдээлэл, цахилгаан соронзон орчныг хамарсан цогц ойлголт гэж үздэг. Энэ олон янзын тайлбар нь “кибер аюулгүй байдал”, “кибер хамгаалалт”, “кибер дайн” зэрэг нэр томьёог оновчтой ялгаж, түүнд үндэслэсэн бодлого, хөтөлбөр боловсруулахад тодорхойгүй байдлыг бий болгож байна.

Кибер сөргөлдөөний хэлбэрийг нарийвчлан үзвэл, кибер гэмт хэрэг, тагнуул, үйлчилгээ тасалдуулах бага нөлөөлөлтэй халдлагаас эхлээд зэвсэгт мөргөлдөөний үед кибер орон зайг хамтад нь ашигласан бүрэн хэмжээний дайн хүртэлх өргөн хүрээтэй болж байна.

Спидальери ба МакАрдел нар бага нөлөөлөлтэй тасралтгүй явагдах зөрчил, халдлагууд нь тайван цагийн зэвсэгт хүчний өдөр тутмын ажилд байнгын ачаалал үүсгэдгийг онцолж, ийм нөхцөлд батлан хамгаалах салбарын боловсон хүчинг бэлтгэдэг боловсролын байгууллага нь кибер орчны онцлогт нийцсэн сургалтын тогтолцоо бүрдүүлэх шаардлагатайг тэмдэглэсэн байдаг.

Иймээс энэ өгүүлэлд кибер орон зай, кибер дайн, кибер цэргийн удирдлага, сургалтын чиг хандлагын уялдаа холбоог системтэйгээр авч үзнэ.

СУДАЛГААНЫ АРГА ЗҮЙ

Энэхүү өгүүлэлд онолын дүн шинжилгээ болон харьцуулсан судалгааны аргыг хослуулан ашигласан. Кибер орон зайг стратегийн домэйн хэмээн авч үзэх үзэл

баримтлал, батлан хамгаалах бодлогын өөрчлөлт, кибер командлалын байгуулалт, сургалтын загваруудыг институцийн түвшинд задлан шинжилж, бодлогын баримт бичиг, байгууллагын шинэчлэлийн мэдээлэл, сургалтын практик жишээ зэрэг анхдагч эх сурвалжид тулгуурлан шинжиллээ.

Харьцуулсан судалгаанд АНУ, НАТО-гийн гишүүн орнуудын жишээ (Европын зарим улс), мөн ОХУ, БНХАУ, Эстони зэрэг кейсийг сонгож, (1) тав дахь домэйн гэж хүлээн зөвшөөрсөн байдал, (2) командлалын эрх хэмжээ ба зохион байгуулалт, (3) сургалтын арга зүй (симуляци, red/blue team, команд-штаб), (4) тасралтгүй чадавхжуулалба хүний нөөцийн бодлого гэсэн шалгууруар харьцуулалт хийв. Судалгааны хязгаарлалт нь зарим улсын довтолгооны кибер чадавхын талаарх мэдээлэл нууцлалтай байдаг тул нийтэд нээлттэй эх сурвалжаар баталгаажих боломжит хүрээнд дүгнэсэн явдал болно.

СУДАЛГААНЫ ҮР ДҮН

Кибер орон зай нь мэдээллийн орчин дахь физик талбар бус, виртуал талбар боловч бодит ертөнцөд ноцтой нөлөөлөл үзүүлэх чадвартай. Энэ нь интернэт, харилцаа холбооны дэд бүтэц, компьютерын сүлжээ зэрэг бүх төрлийн мэдээллийн сүлжээ, төхөөрөмжийн нийлмэл экосистем бөгөөд хүн төрөлхтөн бизнес, санхүү, дэд бүтэц, төрийн удирдлага, цэргийн командлалын ажиллагаагаа энэ орчинд түшиглэн явуулж байна. Кибер орон зайг уламжлалт утгаар газар зүйн байршил, хил хязгаараар зааглах боломжгүй. Халдлага үйлдэгч этгээд байршлаасаа үл хамааран бай болгон онилсон улсынхаа санхүү, эрчим хүч, харилцаа холбоо зэрэг амин чухал дэд бүтцийг доголдуулж, үйлчилгээг нь тасалдуулах, мэдээлэл устгах, хулгайлах замаар улсын аюулгүй байдал болоод хөгжилд шууд нөлөөлж болно. Иймээс ихэнх улс кибер орон зайд өрнөх аливаа үйл явцыг үндэсний хэмжээний аюулгүй байдлын асуудал гэж үзэх болсон. НАТО кибер орон зайг цэргийн ажиллагааны шинэ домайн гэж тунхагласнаар гишүүн орнууд кибер халдлагыг “жинхэнэ” цэргийн халдлагатай адилтган авч үзэх, хамтын хамгаалалтын хүрээнд хариу арга хэмжээ авах боломж бүрдсэн (North Atlantic Treaty Organization 2016). Энэ нь кибер орон зайд үзүүлэх халдлага улс орны бүрэн эрх, тусгаар тогтнолд халдсан үйлдэл байж болохыг хүлээн зөвшөөрч, кибер хамгаалалтын чадавхыг стратегийн түвшинд нэмэгдүүлэх шахалтыг улс орнуудад үзүүлж байна.

Уламжлалт цэргийн онолд газар, тэнгис, агаар (дараа нь сансар) гэх үндсэн тулааны талбаруудыг тодорхойлж ирсэн бол мэдээллийн эрин үед кибер орон зайг тав дахь (зарим тохиолдолд зургаа дахь) дайн тулалдааны талбар гэж үзэх болсон (North Atlantic Treaty Organization 2016). АНУ-ын Батлан хамгаалах яам 2011 оны кибер стратегидаа кибер орон зайг цэргийн үйл ажиллагааны тусгай домайн хэмээн тодорхойлж, тусгайлсан цэргийн хүчнийг зохион байгуулах, сургах, зэвсэглэх шаардлагатай гэж тусгасан нь энэ чиглэлийн суурь баримт бичиг болсон (Department Of Defense Washington Dc 2011). ОХУ мэдээллийн орон зай дахь тэмцлийг онолын түвшинд өргөжүүлэн, “мэдээллийн дайн” гэсэн ойлголтоор кибер ажиллагааг хамтатган авч үзэх болсон. Иймд орчин үеийн цэргийн номлолд кибер орон зай дахь ажиллагаа нь уламжлалт домэйнуудтай ижил стратегийн ач холбогдолтой, олон талбарт ажиллагааны (multi-domain operations) салшгүй хэсэг болж, кибер дайн, мэдээллийн дайн, сүлжээ төвт дайн гэх ойлголтуудыг хэлэлцэх

болсон.

Цэргийн онолын хувьд “домэйн” гэдэг ойлголт нь тухайн орчинд давамгайлал тогтоохын тулд тусгай мэдлэг, чадвар, бүтэц, сургалт шаардагддаг бие даасан талбарыг илэрхийлдэг. Өөрөөр хэлбэл, аливаа орон зайг домэйн гэж хүлээн зөвшөөрөх нь зөвхөн түүнийг ашиглаж болох орчин гэж үзэх бус, харин уг орчинд системтэйгээр бэлтгэгдсэн хүч, тусгайлсан командлал, өөрийн онцлогт тохирсон сургалтын тогтолцоо зайлшгүй шаардлагатайг хүлээн зөвшөөрсөн хэрэг юм.

Энэ утгаараа кибер орон зайг стратегийн домэйн гэж үзэх нь зэвсэгт хүчний уламжлалт бүтэц, номлолд чанарын өөрчлөлт авчирч байна. Хэрэв кибер орон зайг зөвхөн дэмжих хэрэгсэл, эсвэл туслах технологи гэж үзвэл сургалт, хүний нөөцийн бодлого нь дагалдах шинжтэй хэвээр үлдэнэ. Харин бие даасан домэйн хэмээн хүлээн зөвшөөрсөн тохиолдолд кибер орчинд давамгайлал тогтоох, дайсны чадавхыг сулруулах, өөрийн системийг тасралтгүй хамгаалах зорилго бүхий цогц бодлого, зохион байгуулалт шаардагдана.

Иймээс кибер орон зайг домэйн гэж үзэх онолын хандлага нь сургалтын агуулга, хэлбэрийг үндсээр нь өөрчилж, офицер, мэргэжилтнүүдээс зөвхөн техникийн ур чадвар бус, оператив сэтгэлгээ, эрсдэлийн үнэлгээ, команд-штабын түвшний шийдвэр гаргах чадвар шаардах нөхцөлийг бий болгож байна.

Кибер орон зайг хамгаалах, түүнд давуу тал олохын тулд улс орон бүр өөр өөрийн бүтэц, зохион байгуулалтын шийдлүүдийг туршин хэрэгжүүлж байна. Олон улсын туршлагад кибер цэргийг удирдан зохион байгуулах хоёр үндсэн хандлага ажиглагдаж байна. Нэгдүгээрт, бие даасан кибер хүч, командлал байгуулах загвар: Герман улс 2017 онд Kommando Cyber- und Informationsraum[1]-г байгуулж, хуурай зам, тэнгис, агаарын хүчинтэй эн тэнцүү статус бүхий командлал болгосон (Bundesministerium der Verteidigung 2018). Тус командлал цөөн тооны мэдээллийн технологийн мэргэжилтнээс эхэлж, цаашид хэдэн арван мянган цэрэг, энгийн ажилтантай болох зорилт тавьсан нь кибер орон зайг бие даасан стратегийн талбар гэж үзэж буйгаа нотолсон. ОХУ мэдээллийн дайн, кибер ажиллагааны цэргийг байгуулж, улсынхаа мэдээллийн системийг гаднын халдлагаас хамгаалах, давшилтад ашиглах үүргийг ноогдуулсан. Хятад улс 2015 онд Strategic Support Force[2] нэртэйгээр кибер, сансар, цахим дайныг нэгтгэсэн командлал байгуулсан ч 2024 онд бүтцээ задлан, кибер цэргийн хүчийг тусгайлан байгуулж, кибер халдлага, хамгаалалт, тагнуулын үүргийг гүйцэтгүүлэх болсон (Xinhua 2024b; Creemers et al. 2018). Хоёрдугаарт, нэгдмэл, хамтарсан кибер командлалын загвар: АНУ 2009 онд Стратегийн командлалын дор USCYBERCOM (United States Cyber Command)-ыг байгуулж, 2018 онд бие даасан командлалын статустай болгосноор хуурай зам, тэнгис, агаарын бүх салбарын кибер чадавхыг нэг дор удирдах болсон. Командлал тус бүрт байх киберийн нэгжүүд нь USCYBERCOM-д харьяалагдан ажилласнаар олон талбарт ажиллагаанд кибер хүчин давамгай байр суурь эзэлж байна. Эстони улс кибер хамгаалалтын сайн дурын нөөц хүчийг (Cyber Defence Unit) бүрдүүлж, төр-иргэний хамтын загварыг хэрэгжүүлж байна (U.S. Cyber

[1] *Тайлбар: Kommando Cyber- und Informationsraum (KdoCIR) нь Германы Бундесвер (цэргийн хүч)-ний командлал;*

[2] *Тайлбар: Strategic Support Force (SSF) нь Хятадын Ардын Чөлөөлөх Армийн сансар, кибер, мэдээллийн үйл ажиллагааг нэгтгэсэн цэргийн тусгай салбар;*

Command, n.d.). Их Британийн Батлан хамгаалах яам, GCHQ (Government Communications Headquarters)[3]-тэй хамтран довтолгооны кибер ажиллагааны нэгж болох National Cyber Force-ийг байгуулсан нь иргэн-цэргийн хамтарсан загварын жишээ юм (Government Communications Headquarters, 2023).

Кибер орон зайд өрнөх ажиллагааны гол онцлог нь ***цаг хугацааны хязгаар асар богино****, шийдвэр гаргах мөчид мэдээллийн бүрэн бус байдал давамгайлах явдал юм. Иймээс нөхцөлд кибер ажиллагааг уламжлалт зэвсэгт хүчний командлалын шат дамжлагаар дамжуулан удирдах нь хариу арга хэмжээний хурдыг сааруулж, эрсдэлийг нэмэгдүүлэх магадлалтай. Тиймээс олон улс кибер орчныг* ***бие даасан команд-штабын логикоор*** *удирдах шаардлагатай гэж үзэх болсон.*

Кибер командлал байгуулах нь зөвхөн захиргааны шинэ нэгж нэмэх тухай асуудал бус, харин мэдээлэл цуглуулах – үнэлэх – шийдвэр гаргах – хэрэгжүүлэх процессыг нэг төвд төвлөрүүлж, богино хугацаанд гүйцэтгэх институтийн механизм юм. Энэ утгаараа кибер командлал нь хурд, уялдаа холбоо, хариуцлагын тодорхой байдлыг хангах стратегийн хэрэгсэл болж байна.

Бие даасан кибер командлалын загвар нь кибер орчныг бүрэн эрхтэй стратегийн домэйн гэж үздэг орнуудад илүү тохиромжтой. Иймээс загварт кибер ажиллагаа нь хуурай газар, тэнгис, агаарын хүчний адил бие даасан төлөвлөлт, сургалт, хүний нөөцийн бодлоготой байна. Харин нэгдсэн, хамтарсан командлалын загвар нь олон домэйнт ажиллагаанд кибер чадавхыг бусад салбартай нягт уялдуулахад давуу талтай бөгөөд кибер хүчийг “тусгаар” бус, харин ***олон талбарт нөлөөлөх холбогч хүчин*** *болгон ашиглах боломж олгодог.*

Аль ч загварыг сонгосон тохиолдолд кибер командлалын үр ашиг нь түүний ***сургалтын тогтолцоо, мэргэжлийн боловсон хүчний бэлтгэл, шийдвэр гаргах эрх мэдлийн төвлөрөл*** *зэрэг хүчин зүйлээс шууд хамаарна. Иймээс кибер командлалын тухай асуудлыг зөвхөн бүтцийн хүрээнд бус, харин сургалт–хүний нөөц–удирдлагын цогц шинэчлэлийн хүрээнд авч үзэх шаардлагатай.*

Кибер цэргийн ажиллагаа дараах гол шинжээр уламжлалт цэргийн ажиллагаанаас ялгагдана. Үүнд:

- Уламжлалт дайн газар, ус, агаарт физик хил хязгаартай өрнөдөг бол кибер дайн нь физик хил хязгаараас үл хамааран цахим орчинд явагддаг. Үүний зэрэгцээ кибер ажиллагаа нь нуувч, фронтгүй тул уламжлалт дайны тодорхой тулааны шугам гэж үгүй.
- Уламжлалт дайн нь албан ёсоор дайн зарлаж, тодорхой мөчлөгтэйгөөр үргэлжилж төгсдөг бол кибер орон зайд тасралтгүй тэмцэл өрнөж байх тул тайван ба дайны цагийн заагийг бүдгэрүүлж байна.
- Халдлага үйлдэгч этгээдийг тогтоох, хариуцлага тооцох нь техникийн ба хууль эрх зүйн хувьд маш төвөгтэй.
- Кибер дайралт секунд, минутын дотор дэлхийн хаанаас ч олон бай руу зэрэг үйлчилж чаддаг тул хамгаалагч талаас бодит цагийн ойролцоо шийдвэр гаргах чадвар шаарддаг.

Эдгээр онцлог нь уламжлалт стратеги, тактикийг шууд хуулбарлах

[3] *Тайлбар: GCHQ (Government Communications Headquarters) нь Их Британийн тагнуулын гурван үндсэн агентлагийн нэг;*

боломжгүй, кибер орчны онцлогт тохирсон шинэ онол, журам, сургалтын аргачлал шаардлагатайг харуулна. Орчин үеийн зэвсэгт хүчний удирдагчид, шийдвэр гаргагч офицерууд кибер орчинд хэрхэн давуу байх, довтолгооноос сэргийлэх талаар шинэ мэдлэг, тактик боловсруулж, уламжлалт дайны сургаалиудаа дахин сэргээн бичиж байна. АНУ, Япон, Солонгос зэрэг улсууд мэдээллийн технологийн өндөр хөгжилтэй уялдуулан, кибер дайны онол, туршлагыг цэргийн академи, сургалтын хөтөлбөртөө тусган судалж эхлээд байна.

Кибер орон зай дахь аюул заналын хурдтай өсөлт нь цэргийн сургалт, боловсон хүчний хөгжилд шинэ чиг хандлагыг бий болгож байна. Иймээс дэлхийн олон орны батлан хамгаалах байгууллагууд кибер аюулгүй байдлын сургалтын хөтөлбөрөө шинэчилж, дараах чиглэлүүдийг баримталж байна.

Нэгдүгээрт, кибер орчны гол онцлог нь үйл явцын ***хурд, үл харагдах байдал****, мөн нөхцөл байдал богино хугацаанд огцом өөрчлөгдөх шинж чанарт оршдог. Иймээс орчинд кибер халдлагын бодит нөлөө, эрсдэлийг онолын тайлбар, танхимын сургалтаар бүрэн ойлгуулах боломж хязгаарлагдмал байдаг. Иймээс кибер сургалтын арга зүй нь бодит нөхцөлд ойртуулсан, туршлага дээр суурилсан хэлбэрт зайлшгүй шилжих шаардлага үүсдэг.*

Симуляцид суурилсан сургалт нь кибер орчны энэхүү онцлогт хамгийн сайн нийцэх арга зүйд тооцогддог. Учир нь симуляци нь бодит халдлагын явцыг хийсвэрлэн дүрслэх бус, харин ***шийдвэр гаргах дараалал, алдаа гарсан тохиолдолд үүсэх үр дагавар, хариу арга хэмжээний хугацаа*** *зэрэг хүчин зүйлсийг бодитоор мэдрүүлэх боломж олгодог. Энэ нь оролцогчдыг зөвхөн “яаж хийх вэ?” гэдгээс гадна “яагаад ингэж шийдэх ёстой вэ?” гэсэн асуултад хариу хайхад хүргэдэг.*

Red team / blue team-д суурилсан сургалт нь кибер орчны довтолгоо–хамгаалалтын динамикийг ойлгуулах хамгийн үр дүнтэй хэлбэрүүдийн нэг юм. Red team нь бодит дайсны тактик, техник, процедурыг дуурайлган хэрэгжүүлснээр хамгаалалтын сул талыг илрүүлдэг бол blue team нь хамгаалалтын зохион байгуулалт, уялдаа холбоо, хариу арга хэмжээний чадамжийг бодитоор шалгадаг. Энэ төрлийн сургалт нь техникийн ур чадвараас гадна ***багийн ажиллагаа, шийдвэр гаргалтын сахилга бат*** *зэрэг хүний хүчин зүйлийг тодотгож өгдөг.*

Кибер командлалын түвшинд сургалт явуулахад команд-штабын сургалтын ач холбогдол онцгойлон нэмэгддэг. Учир нь бодит кибер халдлагын үед техникийн баг асуудлыг илрүүлсэн ч, ***ямар үед хариу цохилт өгөх, ямар эрсдэлийг хүлээх, улс төр, хууль эрх зүйн үр дагаврыг хэрхэн тооцох*** *зэрэг шийдвэрийг командлагч, удирдагчид гаргадаг. Иймээс кибер сургалт нь зөвхөн инженер, мэргэжилтний түвшинд бус, харин командлалын түвшинд* ***шийдвэр гаргах чадварыг хөгжүүлэх*** *чиглэлтэй байх ёстой.*

Ийнхүү симуляци, red/blue team, команд-штабын сургалт нь хоорондоо уялдсан цогц систем болж, кибер командлалыг бодит ажиллагаанд бэлтгэж, уламжлалт “мэдлэг дамжуулах” хэлбэрээс гарган, ***туршлага бий болгох, чадвар төлөвшүүлэх*** *түвшинд хүргэж байгааг харуулж байна.*

Хоёрдугаарт, кибер орчны технологи, халдлагын тактик, хамгаалалтын арга барил тасралтгүй хувьсан өөрчлөгдөж буй өнөөгийн нөхцөлд нэг удаагийн сургалт нь бодит чадавх бүрдүүлэхэд хангалтгүй болж байна. Өнөөдөр эзэмшсэн

мэдлэг маргаашийн халдлагад шууд тохирохгүй байх эрсдэл өндөр тул кибер чадавх нь ***тогтмол шинэчлэгдэж байх процесс*** *гэж үзэх шаардлагатай. Энэ утгаараа кибер сургалт нь “курс төгсөх” үйл явц бус, харин* ***амьдралын турш үргэлжлэх суралцах замнал*** *болж хувирч байна.*

Тасралтгүй чадавхжуулалт гэдэг нь зөвхөн давтан сургалт зохион байгуулахыг хэлэхгүй. Харин бодит ажиллагаанд оролцох, симуляцид суурилсан дасгалыг тогтмолжуулах, алдаанаас суралцах соёлыг төлөвшүүлэх, мөн шинэ үүрэг гүйцэтгэхийн хэрээр сургалтын агуулгыг шатлан гүнзгийрүүлэх цогц тогтолцоог илэрхийлнэ.Ийм тогтолцоо бүрдээгүй тохиолдолд кибер хүч нь богино хугацаанд чадвартай мэт харагдавч, дунд болон урт хугацаанд чадавх алдах эрсдэлтэй.

Гуравдугаарт, үүнтэй уялдан хүний нөөцийн бодлого кибер чадавхтай салшгүй холбогддог. Өндөр ур чадвартай кибер мэргэжилтэн тогтвортой ажиллахгүй, эсвэл байнга солигдож байвал байгууллагын хуримтлагдсан туршлага алдагдаж, сургалтын үр дүн бодит ажиллагаанд бүрэн шингэх боломж хумигдана. Иймээс олон улс кибер мэргэжилтнүүдийг татах, тогтоон барих асуудлыг цалин, урамшууллын хүрээнээс хальж, ***карьерын уян хатан замнал, мэргэшлийн шаталсан хөгжил, сургалт–алба хаах–ахиц дэвшил*** *хоорондын уялдааг стратегийн түвшинд төлөвлөх болсон.*

Ийнхүү кибер сургалтын шинэчлэл нь практик симуляци, тасралтгүй мэргэшүүлэлт, уян хатан хүний нөөцийн бодлого, олон талт мэдлэг болон хувь хүний сахилга бат хосолсон цогц систем болон төлөвшиж байна.

Дээрх чиг хандлагын бодит хэрэгжилт, үр нөлөө нь гадаадын орнуудын батлан хамгаалах байгууллагуудын туршлагаар тодорхой илэрч байна. Жишээлбэл, АНУ нь 2009 онд Кибер командлалаа байгуулж, 2018 онд бие даасан нэгдсэн командлалын статустай болгосноор кибер хүчнийг зэвсэгт хүчний үндсэн бүрэлдэхүүнд нэгтгэсэн (U.S. Cyber Command, n.d.). Тус улсын кибер бодлого нь төр-хувийн хэвшлийн хамтын ажиллагаанд тулгуурлаж, ISAC (Information Sharing and Analysis Center)[4] мэдээлэл солилцох систем, “CyberStorm” зэрэг бодит нөхцөлд суурилсан сургуулилалтаар дамжуулан төр, боловсрол, технологийн салбарын уялдаа холбоог бий болгосон (Cybersecurity and Infrastructure Security Agency, n.d.). 2010 онд Израилтай хамтран Stuxnet хорт программыг ашиглан Ираны цөмийн байгууламжийг гэмтээсэн (Albright et al. 2010) нь кибер зэвсгийн стратегийн хэрэглээг бодитоор харуулсан бөгөөд өдгөө АНУ “Forward Offensive Cyber” буюу урьдчилан сэргийлэх идэвхтэй хамгаалалтын стратегийг бариманлж байна (U.S. Cyber Command, n.d.). Хүний нөөцийн хувьд Cyber Mission Force байгуулагдсан ч тогтвортой байдлын хүндрэл гарсны улмаас 2025 оноос “Cyber Talent Management Organization”, “Advanced Training Center” -ийг байгуулж, тасралтгүй сургалт ба уян хатан карьерын системийг хэрэгжүүлж эхэлсэн.

НАТО Эстони дахь CCDCOE (Cooperative Cyber Defence Centre of Excellence) төвийг өргөтгөн, жил бүрийн Locked Shields дасгал сургуулиар (NATO Cooperative Cyber Defence Centre of Excellence, n.d.) гишүүн орнуудын red team / blue team багуудыг бодит халдлагын орчинд дадлагажуулдаг (NATO Cooperative Cyber

[4] *Тайлбар: ISAC гэдэг нь кибер аюул заналхийллийн мэдээллийг салбар бүрийн байгууллагуудын хооронд хуваалцаж, шинжилдэг хамтын ажиллагааны байгууллага;*

Defence Centre of Excellence, n.d.). Энэ нь командлалын түвшинд шийдвэр гаргах чадвар, олон улсын кибер хамтын ажиллагааг хөгжүүлэх хамгийн том практик симуляци болдог.

Европын орнуудаас Герман, Их Британи, Франц зэрэг улс кибер офицер бэлтгэх академи, судалгааны хүрээлэнг байгуулж, стратеги, хууль эрх зүй, менежментийн мэдлэгийг техник-тактикийн сургалттай хослуулсан олон талт хөтөлбөрийг нэвтрүүлж байна.

ОХУ кибер орон зайг батлан хамгаалах бодлогоос тусгаар бус, стратегийн мэдээллийн дайнтай уялдуулсан байдлаар хөгжүүлж, 2012 онд Батлан хамгаалах яамны харьяанд цэргийн академи байгуулсан. Энэ байгууллага нь кибер халдлага, мэдээллийн нөлөөллийн ажиллагаа, сэтгэлзүйн дайн, хуурамч мэдээлэлд хариу арга хэмжээ авах сургалтыг хослуулсан “мэдээллийн дайны цогц” хөтөлбөрөөр офицеруудыг сургаж байна. Оросын сургалтын онцлог нь “defensive–offensive integration” буюу хамгаалалт, довтолгооны чадварыг нэгэн зэрэг хөгжүүлэх зарчмыг баримталдагт байгаа юм.

Харин БНХАУ кибер орон зайг үндэсний аюулгүй байдлын тулгуур чиглэл хэмээн үзэж, 2015 онд “Network Security Law”-оо баталснаар төрийн хяналтад суурилсан кибер хамгаалалтын нэгдсэн тогтолцоог бүрдүүлсэн (Xinhua 2024a; Creemers et al. 2018). Хятадын Ардын Чөлөөлөх Армийн Стратегийн хүч (Xinhua 2024b) нь кибер, сансрын болон цахим тагнуулын үйл ажиллагааг нэгтгэн, “интеграцчилсан сүлжээний дайн”-ы үзэл баримтлалд тулгуурлан сургалт, судалгааг хөгжүүлж байна. Мөн Циньхуа, Харбин инженерийн их сургууль зэрэг боловсролын байгууллагуудад кибер офицер, хамгаалалтын инженер бэлтгэх цэргийн хөтөлбөр хэрэгжиж, төр-хувийн хэвшлийн лаборатори, инновацын төвүүдтэй нягт уялдаатай ажиллаж байна.

Ийнхүү АНУ, НАТО, Европ, Орос, Хятадын туршлагаас харахад кибер сургалт нь улс төр, батлан хамгаалах бодлого, технологийн хөгжилтэй нягт уялдсан стратегийн шинжтэй үйл ажиллагаа болж, хүн төвтэй тасралтгүй сургалт, бодит нөхцөлд суурилсан бэлтгэл, төр-хувийн хэвшлийн хамтын ажиллагаа, мэдээллийн дайн ба хууль эрх зүйн орчныг хослуулсан иж бүрэн тогтолцоонд шилжиж байна.

Батлан хамгаалах салбарын уламжлал сургаал, номлолд эрс өөрчлөлтийг авчирсан кибер орон зайн аюулгүй байдлыг хангахын тулд улс орнууд батлан хамгаалах салбартаа дараах өөрчлөлт, шинэчлэлийг хийх нь зохимжтой юм. Үүнд:

- Кибер цэргийн чадавхаа бэхжүүлэхийн тулд бие даасан кибер хүчин байгуулах эсвэл нэгдсэн командлалын загварыг хэрэгжүүлэн зохион байгуулалтын шинэ хэлбэр турших.
- Улс орны батлан хамгаалах чадавхад тохирсон шинэ онол, тактик, шийдвэр гаргалт, сургалтын аргачлалыг хөгжүүлэх.
- Бодит халдлагын нөхцөлд суурилсан симуляц, дадлагад суурилсан практик төвтэй сургалтын загварт эрчимтэй шилжих.
- Хурдтай хувьсалыг дагаад тасралтгүй мэргэшүүлэх, модульчилсан сургалтыг зохион байгуулах.
- Өндөр ур чадвартай кибер мэргэжилтнийг татах, тогтоон барихын тулд уян хатан гэрээ, урамшуулал, карьерын өсөлт бүхий хүний нөөцийн шинэ бодлого

хэрэгжүүлэх.

- Хувь хүний кибер сахилга батыг нэмэгдүүлэх сургалт, шалгалтын тогтолцоог тогтвортой хэрэгжүүлэх.
- Кибер сургалтыг дан техник бус, бодлого, хууль эрх зүй, мэдээллийн дайн, технологийн инновацыг уялдуулсан иж бүрэн стратегийн тогтолцоо болох чиглэлд анхаарал хандуулах.

ХЭЛЭЛЦҮҮЛЭГ

Энэхүү өгүүлэлд гарсан гол ажиглалт нь кибер чадавхыг “техникийн шинэчлэл” гэж хязгаарлах үед сургалт, хүний нөөц, командлалын шинэчлэл салангид хэрэгжиж, бодит ажиллагааны үр нөлөө сулрах хандлага юм. Харин кибер орон зайг домэйн гэж институцийн түвшинд хүлээн зөвшөөрсөн тохиолдолд командлалын эрх хэмжээ тодорхой болж, сургалтын зорилго нь зөвхөн хэрэгсэл эзэмшүүлэхээс “оператив шийдвэр гаргалт”-ын чадварыг хөгжүүлэх чиглэл рүү шилждэг.

Мөн симуляцид суурилсан сургалт, red team/blue team дасгал, команд-штабын сургалт гурвыг тус тусад нь бус, харин нэг экосистем болгож тогтмолжуулах үед сургалтын өгөөж бодит чадавх болж хөрвөх боломж илүү өндөр байдаг нь олон улсын туршлагаас харагдаж байна. Тухайлбал, техникийн баг халдлагыг илрүүлсэн ч хариу арга хэмжээний зөвшөөрөл, эрсдэлийн сонголт, хууль-улс төрийн үр дагаврыг тооцох шийдвэрийг командлагч, штабын түвшин гаргадаг учир сургалтын зорилтот түвшин зөвхөн инженерүүдээр хязгаарлагдах боломжгүй.

Гэхдээ “ганц зөв загвар” гэж байхгүй. Зарим улс бие даасан кибер командлалын загвараар домэйн статусыг баталгаажуулсан бол, зарим нь нэгдсэн хамтарсан удирдлагын загвараар олон домэйнт ажиллагаатай уялдуулах давуу талыг сонгож байна. Энэ ялгаа нь улс төр-удирдлагын тогтолцоо, стратегийн сонирхол, нөөцийн багтаамжаас хамаарах боловч аль аль тохиолдолд “тодорхой эрх мэдэл + тасралтгүй сургалт + тогтвортой хүний нөөц” гэсэн гурвалсан шаардлага нийтлэг хүчин зүйл болж байна.

ДҮГНЭЛТ

Кибер орон зайг бие даасан стратегийн домэйн хэмээн авч үзэх нь батлан хамгаалах салбарын удирдлага, сургалт, хүний нөөцийн бодлогыг цогцоор нь өөрчлөх шаардлага үүсгэж байна. Судалгааны хүрээнд кибер чадавх нь зөвхөн техник-технологийн шинэчлэлээр бүрдэхгүй бөгөөд (1) хурдан шийдвэр гаргах эрх хэмжээ тодорхой командлалын зохион байгуулалт, (2) симуляци–red/blue team–команд-штабын сургалтад суурилсан практик төвтэй сургалтын экосистем, (3) тасралтгүй чадавхжуулалтыг дэмжих уян хатан хүний нөөцийн бодлого гэсэн гурван тулгуур хүчин зүйлийн харилцан тэнцвэрт өсөлтөөс хамааралтай юм. Иймээс кибер орчны давуу байдлыг хангах тогтвортой зам нь институц, сургалт, хүний хүчин зүйлийг нэгэн зэрэг хөгжүүлэх интеграцчилсан хандлага хэмээн үзэж байна.

Эшлэл авсан сурвалж, судалгааны бүтээл:

1. Albright, David, Paul Brannan, and Christina Walrond. 2010. *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment*.

Institute for Science and International Security. https://isis-online.org/isis-reports/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant.
2. Bundesministerium der Verteidigung. 2018. *7. Bericht Des Bundesministeriums Der Verteidigung Zu Rüstungsangelegenheiten, Teil 1*. Bundesministerium der Verteidigung. https://www.bmvg.de/resource/blob/23010/7362820057116c6763aaec84147ce3ea/20180319-7-bericht-des-bmvg-zu-ruestungsangelegenheiten-data.pdf.
3. Creemers, Rogier, Graham Webster, and Paul Triolo. 2018. “Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017).” DigiChina, Stanford University Cyber Policy Center, June 29. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.
4. Cybersecurity and Infrastructure Security Agency. n.d. “Cyber Storm: Securing Cyber Space.” U.S. Department of Homeland Security. Accessed July 7, 2026. https://www.cisa.gov/resources-tools/programs/cyber-storm.
5. Department Of Defense Washington Dc. 2011. *Department of Defense Strategy for Operating in Cyberspace:* Defense Technical Information Center. https://doi.org/10.21236/ADA546341.
6. Government Communications Headquarters. 2023. “National Cyber Force Reveals How Daily Cyber Operations Protect the UK.” GOV.UK, April 4. https://www.gov.uk/government/news/national-cyber-force-reveals-how-daily-cyber-operations-protect-the-uk.
7. NATO Cooperative Cyber Defence Centre of Excellence. n.d. “Locked Shields.” Accessed July 7, 2026. https://ccdcoe.org/locked-shields/.
8. North Atlantic Treaty Organization. 2016. *Warsaw Summit Communiqué*. Communiqué. North Atlantic Treaty Organization. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique.
9. U.S. Cyber Command. n.d. “Command History.” Accessed July 7, 2026. https://www.cybercom.mil/About/History/.
10. Xinhua. 2024a. “PLA’s Information Support Force Is Brand-New Strategic Arm: Defense Spokesperson.” Xinhuanet, April 19. https://english.news.cn/20240419/2b64c22c5e8742d4949e0a923f6dc68f/c.html.
11. Xinhua. 2024b. “Xi Presents Flag to PLA’s Information Support Force.” The State Council of the People’s Republic of China, April 19. https://english.www.gov.cn/news/202404/19/content_WS66225707c6d0868f4e8e63bd.html.