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.2026.02.007

Developing Smart Defence in Mongolia: Trends in the Reform of Defence Education

Zagdsuren Boldbaatar[1], Boldbaatar Amartur[2]

[1]Sc.D., Professor, Senior Researcher, Security studies center, Defense research Institute of Mongolia
E-mail address: boldbaatar.zagdsuren@gmail.com
[2]Researcher, Center for defense research, Defense research Institute of Mongolia
E-mail address: amartur.boldbaatar@gmail.com, ORCID: 0009-0009-2801-6753

Received: 07 June 2026 *Revised: 22 June 2026*
Accepted: 30 June 2026 *Published online: 28 July 2026*

ABSTRACT

The rapidly evolving security environment, characterized by geopolitical competition, cyber threats, artificial intelligence (AI), and autonomous systems, requires new approaches to defence modernization. For resource-constrained countries such as Mongolia, Smart Defence provides a practical framework for enhancing military capability through technological innovation, efficient resource utilization, and institutional adaptation.

This study examines the theoretical foundations of Smart Defence and assesses its applicability to Mongolia through comparative analysis, case studies, and document analysis of selected international experiences. The findings indicate that Mongolia should prioritize cyber defence, artificial intelligence, unmanned systems, information security, and digital command-and-control capabilities while strengthening defence education as the foundation of military modernization.

Accordingly, the study proposes a Smart Defence Education Model tailored to Mongolia's national conditions by integrating emerging disciplines—including artificial intelligence, cyber security, open-source intelligence, drone operations, and cognitive warfare—into military education. The proposed model provides a practical framework for defence policy development, military education reform, and the long-term modernization of Mongolia's national defence system.

Keywords: *Smart Defence; Military Modernization; Artificial Intelligence; Defence Innovation; Defence Education.*

Ухаалаг батлан хамгаалалтыг хөгжүүлэх нь: Батлан хамгаалах боловсролын шинэ чиг хандлага

Загдсүрэн Болдбаатар[1], Болдбаатар Амартөр[2]

[1]Батлан хамгаалах эрдэм шинжилгээний хүрээлэнгийн Аюулгүй байдал судлалын төвийн ахлах судлаач доктор (Sc.D), профессор, boldbaatar.zagdsuren@gmail.com
[2]Батлан хамгаалах эрдэм шинжилгээний хүрээлэнгийн Батлан хамгаалах судлалын төвийн эрдэм шинжилгээний ажилтан, магистр, amartur.boldbaatar@gmail.com, ORCID: 0009-0009-2801-6753

ХУРААНГУЙ

Геополитикийн өрсөлдөөн, кибер аюул занал, хиймэл оюун, автономит систем зэрэг технологийн хурдацтай хөгжил нь орчин үеийн аюулгүй байдлын орчныг эрс өөрчилж, батлан хамгаалах тогтолцоог шинэчлэх шаардлагыг улам бүр нэмэгдүүлж байна. Нөөц боломж харьцангуй хязгаарлагдмал Монгол Улсын хувьд ухаалаг батлан хамгаалалт нь технологийн инновац, нөөцийн оновчтой ашиглалт, байгууллагын дасан зохицох чадварт тулгуурлан батлан хамгаалах чадавхыг бэхжүүлэх бодитой арга зам юм.

Энэхүү судалгаанд ухаалаг батлан хамгаалалтын онолын үндсийг авч үзэж, олон улсын туршлагад харьцуулсан шинжилгээ, кейс судалгаа болон баримт бичгийн шинжилгээний аргыг ашиглан Монгол Улсад хэрэгжүүлэх боломжийг үнэлэв. Судалгааны үр дүнгээс үзэхэд Монгол Улс батлан хамгаалах шинэчлэлийн хүрээнд кибер аюулгүй байдал, хиймэл оюун, нисгэгчгүй систем, мэдээллийн аюулгүй байдал, дижитал команд удирдлагын чадавхыг тэргүүлэх чиглэл болгон хөгжүүлэхийн зэрэгцээ батлан хамгаалах боловсролыг шинэчлэлийн суурь хүчин зүйл болгон хөгжүүлэх шаардлагатай байна.

Үүний үндсэн дээр Монгол Улсын нөхцөлд нийцсэн “Ухаалаг батлан хамгаалах боловсролын загвар”-ыг санал болгож, хиймэл оюун, кибер аюулгүй байдал, нээлттэй эх сурвалжийн тагнуул, дроны ажиллагаа, танин мэдэхүйн дайны чиглэлийг цэргийн боловсролд үе шаттайгаар нэвтрүүлэх арга замыг тодорхойлов. Судалгааны үр дүн нь батлан хамгаалах бодлого, цэргийн боловсролын шинэчлэл, Монгол Улсын батлан хамгаалах тогтолцооны урт хугацааны шинэчлэлд практик ач холбогдолтой.

Түлхүүр үг: *Ухаалаг батлан хамгаалах загварчлал; Цэргийн шинэчлэл; Хиймэл оюун; Кибер аюулгүй байдал; Батлан хамгаалах инновац; Батлан хамгаалах боловсрол;.*

ОРШИЛ

XXI зууны олон улсын аюулгүй байдлын орчин нь геополитикийн өрсөлдөөн, кибер халдлага, мэдээллийн дайн, хиймэл оюун, автономит систем зэрэг технологийн хурдацтай хөгжлийн нөлөөгөөр үндсээрээ өөрчлөгдөж байна. Үүний зэрэгцээ уламжлалт цэргийн хүчин чадалд тулгуурласан батлан хамгаалах загварын үр ашиг буурч, технологи, инновац, мэдээллийн давуу тал, өндөр ур чадвартай хүний нөөцөд суурилсан хөгжлийн чиг хандлага дэлхий нийтэд эрчимтэй төлөвшиж байна (Bisogniero 2011).

Энэхүү өөрчлөлтийн хүрээнд олон улс хязгаарлагдмал төсөв, нөөц боломжийг илүү үр ашигтай ашиглах зорилгоор “Ухаалаг батлан хамгаалах” (Smart Defence) үзэл баримтлалыг батлан хамгаалах бодлого, төлөвлөлтийн шинэ чиглэл болгон хэрэгжүүлж байна. НАТО 2011 онд Ухаалаг Батлан хамгаалах санаачлагыг хэрэгжүүлж эхэлснээр энэхүү үзэл баримтлал нь технологийн шинэчлэл, хамтын ажиллагаа, нөөцийн оновчтой ашиглалтад тулгуурласан батлан хамгаалах хөгжлийн олон улсын жишиг хандлага болсон (NATO, Madrid Summit Declaration 2022).

Орчин үеийн зэвсэгт мөргөлдөөнүүд, тухайлбал Орос–Украйны дайн болон Израиль–Хамасын мөргөлдөөн нь хиймэл оюун, нисгэгчгүй систем, кибер хамгаалалт, сүлжээ төвт удирдлага зэрэг технологид суурилсан чадавх байлдааны үр дүнг тодорхойлох хүчин зүйл болсныг харуулж байна (Clausewitz 1984). Иймд нөхцөлд Монгол Улс өргөн уудам нутаг дэвсгэр, хүн амын нягтаршил багатай байдал, эдийн засгийн харьцангуй хязгаарлагдмал нөөц, геостратегийн онцлог зэрэг хүчин зүйлээ харгалзан уламжлалт тоон давуу талд бус, өндөр үр ашигтай, технологид суурилсан батлан хамгаалах чадавхыг хөгжүүлэх шаардлагатай болж байна (Alvin Toffler 1994).

Иймээс ухаалаг батлан хамгаалах загварчлал нь Монгол Улсын хувьд зөвхөн цэргийн технологийн шинэчлэлийн асуудал бус, батлан хамгаалах бодлого, боловсрол, судалгаа, инновац, хүний нөөцийн хөгжлийг цогцоор нь шинэчлэх стратегийн чиглэл юм. Энэхүү судалгаа нь ухаалаг батлан хамгаалалтын онолын үндсийг тодорхойлж, олон улсын туршлагыг харьцуулан шинжилсний үндсэн дээр Монгол Улсын батлан хамгаалах боловсролын шинэчлэлийн чиглэл, хэрэгжүүлэх боломжтой хөгжлийн загварыг санал болгохыг зорилоо (Creveld 1991).

УХААЛАГ БАТЛАН ХАМГААЛАЛТЫН ОНОЛЫН ҮНДЭС

Ухаалаг батлан хамгаалах үзэл баримтлалын үүсэл ба хөгжил

Хүйтэн дайны дараах олон улсын аюулгүй байдлын орчинд терроризм, кибер халдлага, мэдээллийн дайн, зохион байгуулалттай гэмт хэрэг, бүс нутгийн тогтворгүй байдал зэрэг уламжлалт бус аюул занал эрчимтэй нэмэгдэж, батлан хамгаалах бодлого, төлөвлөлтийн арга барилыг үндсээр нь өөрчлөх шаардлагыг бий болгосон. Үүнтэй зэрэгцэн дэлхийн санхүү, эдийн засгийн хямралын улмаас батлан хамгаалах төсөв хумигдаж, улс орнууд, ялангуяа НАТО-гийн гишүүд, хязгаарлагдмал нөөцөөр хамгаалалтын үр ашгаа нэмэгдүүлэх шинэ арга зам эрэлхийлэх болсон нь “Ухаалаг батлан хамгаалах” (Smart Defence) үзэл баримтлал төлөвших үндсэн нөхцөл болсон юм (RAND Corporation 2001).

Үүний хүрээнд НАТО 2011 онд Ухаалаг Батлан хамгаалах санаачилгыг хэрэгжүүлж эхэлснээр батлан хамгаалах салбарын шинэчлэлийн тэргүүлэх үзэл баримтлалын нэг болсон. Үүний гол зорилго нь технологийн шинэчлэл, олон улсын хамтын ажиллагаа, нөөцийн оновчтой хуваарилалтыг уялдуулан хязгаарлагдмал хөрөнгө, боломжийн хүрээнд хамгаалалтын чадавхыг нэмэгдүүлэхэд оршиж байгаа юм.

Ухаалаг батлан хамгаалах үзэл баримтлал нь нөөцийг оновчтой ашиглах, улс орнуудын харьцангуй давуу талд тулгуурласан мэргэшлийг хөгжүүлэх, хиймэл оюун, автоматжуулалт, кибер хамгаалалт, том өгөгдөл зэрэг дэвшилтэт технологийг батлан хамгаалах салбарт үр ашигтай нэвтрүүлэх, мөн олон улсын хамтын ажиллагаа, мэдээлэл солилцоо, нэгдсэн чадавхыг хөгжүүлэх үндсэн зарчимд тулгуурладаг. Ийм хандлага нь ижил төрлийн өндөр өртөгтэй чадавхыг улс бүр тусад нь хөгжүүлэхээс илүүтэйгээр хамтын ажиллагаанд суурилсан, үр ашигтай хамгаалалтын тогтолцоог бүрдүүлэх боломжийг бий болгож байна (Rid 2013).

Ийнхүү ухаалаг батлан хамгаалах загварчлал нь зөвхөн цэргийн шинэчлэлийн хүрээний ойлголт бус, боловсрол, шинжлэх ухаан, технологи, инновац, институцийн хөгжлийг батлан хамгаалах бодлоготой уялдуулсан стратегийн хөгжлийн цогц үзэл баримтлал болон хувьсан хөгжиж байна. Орчин үеийн аюулгүй байдлын орчинд энэхүү үзэл баримтлал нь ялангуяа нөөц боломж хязгаарлагдмал улс орнуудын батлан хамгаалах чадавхыг урт хугацаанд тогтвортой хөгжүүлэх бодлогын чухал үндэс болж байна.

Сүлжээ төвт дайны онол ба ухаалаг батлан хамгаалах загварчлал

Ухаалаг батлан хамгаалах загварчлалын онолын суурь үзэл баримтлалын нэг нь “**сүлжээ төвт дайн**” (Network-Centric Warfare, NCW) юм. Энэхүү онолыг 1990-ээд оны сүүлээр АНУ-ын батлан хамгаалахын судлаачид боловсруулсан

бөгөөд мэдээллийн технологийг байлдааны ажиллагаатай уялдуулан командлал, удирдлага, шийдвэр гаргалтын үр ашгийг дээшлүүлэхэд чиглэж байв (Singer 2009). сүлжээ төвт дайны үндсэн санаа нь мэдээллийн давуу байдлыг байлдааны давуу тал болгон хувиргах явдал бөгөөд мэдрэгч (sensor), холбооны сүлжээ (network), шийдвэр гаргалт (decision), ажиллагаа (action) гэсэн тасралтгүй мөчлөгийг хамгийн богино хугацаанд хэрэгжүүлж чадсан тал байлдааны ажиллагаанд илүү өндөр үр ашигтай байх боломжтой гэж үздэг.

Энэхүү үзэл баримтлалын хүрээнд мэдээлэл цуглуулах систем, холбооны сүлжээ, команд удирдлагын төв, байлдааны нэгжүүдийг нэгдсэн мэдээллийн орчинд холбосноор нөхцөл байдлын нэгдсэн ойлголт (Common Operational Picture) бүрдэж, шийдвэр гаргах хугацаа эрс богиносохын зэрэгцээ ажиллагааны уялдаа, нарийвчлал, үр ашиг мэдэгдэхүйц нэмэгддэг (Henry A Kissinger 2021). Орчин үеийн зэвсэгт мөргөлдөөнүүдэд дрон, хиймэл дагуул, цахим тагнуул болон бусад эх сурвалжаас цугларсан мэдээллийг бодит цагийн горимд нэгтгэн боловсруулах нь байлдааны үр дүнд шууд нөлөөлөх болсон нь энэхүү онолын практик ач холбогдлыг улам бүр тодотгож байна.

Иймээс сүлжээ төвт дайны онол нь ухаалаг батлан хамгаалалтын технологийн үндэс төдийгүй, хиймэл оюун, кибер хамгаалалт, нисгэгчгүй систем, өгөгдөлд суурилсан команд удирдлагыг нэгтгэсэн орчин үеийн батлан хамгаалах тогтолцоог хөгжүүлэх онолын суурь болж байна. Монгол Улсын хувьд энэхүү хандлага нь хязгаарлагдмал нөөцөөр мэдээллийн давуу тал, технологийн чадавхад тулгуурласан батлан хамгаалах чадавхыг хөгжүүлэх стратегийн ач холбогдолтой юм.

Хиймэл оюун ба батлан хамгаалахын технологийн хувьсгал

Дөрөв дэх аж үйлдвэрийн хувьсгалын гол хөдөлгөгч хүч болсон хиймэл оюун, автоматжуулалт, робот техник, том өгөгдөл, үүлэн тооцоолол, квант технологи зэрэг дэвшилтэт технологиуд нь батлан хамгаалах салбарын хөгжлийн логик, байлдааны арга хэлбэрийг үндсээр нь өөрчилж байна (U.S. Department of Defense 2022). Орчин үеийн цэргийн ажиллагаанд хиймэл оюун нь их хэмжээний мэдээллийг богино хугацаанд боловсруулах, нөхцөл байдлыг үнэлэх, шийдвэр гаргалтыг дэмжих, кибер халдлагыг илрүүлэх, логистикийг оновчлох, нисгэгчгүй системүүдийн ажиллагааг удирдах зэрэг олон чиглэлээр ашиглагдаж, командлал, удирдлагын үр ашиг болон ажиллагааны хурдыг мэдэгдэхүйц нэмэгдүүлж байна.

Сүүлийн жилүүдийн зэвсэгт мөргөлдөөнүүд, ялангуяа Орос–Украйны дайн нь харьцангуй хямд өртөгтэй FPV дрон, хиймэл оюунд суурилсан тандалт, өгөгдлийн бодит цагийн боловсруулалт зэрэг технологиуд өндөр үнэтэй уламжлалт зэвсэглэлийн эсрэг үр ашигтай болохыг харуулж, байлдааны хүчний талаарх уламжлалт ойлголтыг өөрчилсөн. Үүний зэрэгцээ АНУ Joint All-Domain Command and Control (JADC2) буюу **бүх ажиллагааны орчны нэгдсэн команд удирдлагын тогтолцоо**, БНХАУ Intelligentized Warfare буюу “Ухаалагжсан дайн”, Израиль AI-enabled Warfare буюу хиймэл оюунд суурилсан дайн зэрэг үзэл баримтлалыг хөгжүүлэн хиймэл оюуныг команд удирдлага, байлдааны төлөвлөлт, мэдээллийн давуу байдлыг бий болгох үндсэн хэрэгсэл болгон ашиглах бодлогыг эрчимтэй хэрэгжүүлж байна.

Гэвч хиймэл оюуныг батлан хамгаалах салбарт өргөн хүрээнд нэвтрүүлэхийн

хэрээр алгоритмын ил тод байдал, хүний хяналтын түвшин, хариуцлагын асуудал, ёс зүйн зохицуулалт, кибер эмзэг байдал зэрэг шинэ сорилтууд мөн нэмэгдэж байна. Иймээс хиймэл оюунд суурилсан батлан хамгаалах тогтолцоог хөгжүүлэхдээ зөвхөн технологийн чадавхыг бус, эрх зүй, ёс зүй, институцийн зохицуулалт, хүний нөөцийн бэлтгэлийг цогцоор нь авч үзэх шаардлагатай бөгөөд энэ нь ухаалаг батлан хамгаалалтын тогтолцооны тогтвортой хөгжлийн үндсэн нөхцөл болж байна (NATO. Cooperative Cyber Defense Centre of Excellence 2023).

УХААЛАГ БАТЛАН ХАМГААЛАЛТЫН ОЛОН УЛСЫН ТУРШЛАГА БА СУРГАМЖ

НАТО-гийн ухаалаг батлан хамгаалалтын загвар

НАТО 2011 онд Ухаалаг батлан хамгаалах санаачилгыг хэрэгжүүлснээр батлан хамгаалах салбар дахь хамтын ажиллагаа, нөөцийн оновчтой ашиглалт, технологийн шинэчлэлийг аюулгүй байдлын бодлогын тэргүүлэх чиглэл болгон тодорхойлсон. Энэхүү санаачилга нь 2008 оны дэлхийн санхүүгийн хямралын дараах төсвийн хязгаарлалтад хариу болгон бий болсон бөгөөд хязгаарлагдмал нөөцөөр илүү өндөр хамгаалалтын чадавх бүрдүүлэхэд чиглэж байв. Энэ хүрээнд агаарын тандалт, пуужингийн довтолгооноос хамгаалах систем, кибер хамгаалалтын төв, стратегийн тээвэрлэлтийн зэрэг өндөр өртөгтэй чадавхуудыг хамтран хөгжүүлж, Балтын орнуудын агаарын орон зайн хамгаалалтын тогтолцоо зэрэг амжилттай загваруудыг хэрэгжүүлсэн байна. Монгол Улсын хувьд энэхүү туршлага нь давхардсан чадавхыг бууруулах, олон улсын хамтын ажиллагааг өргөжүүлэх, энхийг дэмжих ажиллагаа болон кибер хамгаалалтын чиглэлээр хамтарсан сургалт, дадлагыг хөгжүүлэхэд бодитой ач холбогдолтой.

АНУ, БНХАУ-ын технологид суурилсан батлан хамгаалах шинэчлэл

АНУ болон БНХАУ нь хиймэл оюун, том өгөгдөл, кибер орон зай, сансар, нисгэгчгүй системийг батлан хамгаалах хөгжлийн үндсэн чиглэл болгон тодорхойлж, мэдээлэлд суурилсан команд удирдлагын шинэ тогтолцоог бүрдүүлэхэд төвлөрч байна. АНУ Joint All-Domain Command and Control (JADC2) буюу бүх ажиллагааны орчны нэгдсэн команд удирдлагын тогтолцоо, Project Maven, Replicator Initiative, Chief Digital and Artificial Intelligence Office (CDAO) зэрэг хөтөлбөрөөр дамжуулан өгөгдөлд суурилсан шийдвэр гаргалт, хиймэл оюуны хэрэглээг эрчимтэй хөгжүүлж байгаа бол БНХАУ “Ухаалагжсан дайн” (Intelligentized Warfare) үзэл баримтлалын хүрээнд хиймэл оюунд суурилсан командлал, дроны сүрэг, том өгөгдлийн боловсруулалт, квант холбоо, хиймэл дагуулын нэгдсэн систем, цэрэг–иргэний интеграцыг хөгжүүлж байна. Эдгээр туршлагаас үзэхэд батлан хамгаалах шинэчлэл нь зөвхөн шинэ техник худалдан авах асуудал бус, технологи, шинжлэх ухаан, боловсрол, судалгаа, хувийн хэвшлийн хамтын ажиллагааг нэгтгэсэн үндэсний инновацын тогтолцоонд тулгуурлах шаардлагатай байна.

Израилийн өндөр технологид суурилсан хамгаалалтын загвар

Израиль улс газар нутгийн хэмжээ харьцангуй бага боловч аюулгүй байдлын өндөр эрсдэлтэй орчинд технологид суурилсан хамгаалалтын тогтолцоог амжилттай хөгжүүлсэн жишээ юм. Iron Dome пуужингийн довтолгооноос хамгаалах систем, үндэсний кибер хамгаалалт, батлан хамгаалах стартап экосистем,

цэрэг–их сургууль–үйлдвэрлэлийн хамтын ажиллагаа, тагнуулын мэдээллийн нэгдсэн тогтолцоо зэрэг нь тус улсын хамгаалалтын чадавхын үндэс болж байна. Израилийн туршлагаас харахад хүний нөөцийн чанар, судалгаа, инновацын тогтолцоо нь жижиг улсын аюулгүй байдлыг хангах стратегийн гол хүчин зүйл бөгөөд Монгол Улсын хувьд их сургууль, судалгааны хүрээлэнд түшиглэсэн батлан хамгаалах судалгаа, инновацын төвийг хөгжүүлэх шаардлагатайг харуулж байна.

Жижиг улсын батлан хамгаалах шинэчлэлийн туршлага

Монгол Улстай хүн ам, нөөц боломж, аюулгүй байдлын орчны зарим онцлог талаар төстэй Эстон, Финланд, Швейцарь зэрэг улсын туршлага нь ухаалаг батлан хамгаалалтыг хөгжүүлэхэд бодитой сургамж өгч байна. Эдгээр улс нь уламжлалт цэргийн хүчийг дангаар нь нэмэгдүүлэхээс илүүтэйгээр кибер хамгаалалт, өндөр бэлтгэлтэй нөөц хүчин, иргэн–цэргийн хамтын ажиллагаа, үндэсний тэсвэрлэх чадвар, дэвшилтэт технологид тулгуурласан хамгаалалтын тогтолцоог хөгжүүлснээр хязгаарлагдмал нөөцөөр өндөр үр ашигтай батлан хамгаалах чадавхыг бүрдүүлжээ.

Эстон улс 2007 оны өргөн хүрээний кибер халдлагын дараа үндэсний кибер командлал, кибер нөөц хүчин, цахим засаглал, кибер боловсролыг хөгжүүлэн дэлхийд тэргүүлэх кибер хамгаалалтын загваруудын нэг болсон (Czosseck 2011). Финланд улс “**Comprehensive Security**” буюу бүх нийтийн аюулгүй байдлын үзэл баримтлалын хүрээнд төр, хувийн хэвшил, иргэдийн хамтын оролцоо, өндөр бэлтгэлтэй нөөц хүчин, орон нутгийн хамгаалалт, кибер аюулгүй байдлыг нэгдсэн тогтолцоонд хөгжүүлж байна (Committee Security 2023). Харин Швейцарь улс төвийг сахих бодлогоо хадгалсан хэдий ч милицийн зарчимд суурилсан нөөц хүч, төвлөрлийг сааруулсан команд удирдлага, иргэн–цэргийн уялдаа холбоог үр ашигтай хөгжүүлснээр үндэсний батлан хамгаалах тогтолцооны тогтвортой байдлыг хангаж байна.

Эдгээр улсын туршлагаас харахад жижиг, дунд хэмжээний улс орнуудын батлан хамгаалах чадавх нь зөвхөн зэвсэглэл, техник хэрэгслийн хэмжээгээр бус, кибер хамгаалалт, боловсрол, үндэсний тэсвэрлэх чадвар, нөөц хүчний бэлтгэл, инновацын тогтолцоогоор тодорхойлогдох болсон байна. Монгол Улсын хувьд эдгээр туршлагыг үндэсний нөхцөлд нийцүүлэн нутагшуулах нь ухаалаг батлан хамгаалалтын тогтолцоог хөгжүүлэх бодлогын чухал чиглэл гэж үзэж болно.

Ухаалаг батлан хамгаалалтын сургамж

Олон улсын туршлагын харьцуулсан шинжилгээнээс үзэхэд хүн ам цөөн, нөөц боломж хязгаарлагдмал улс орнууд батлан хамгаалах чадавхаа уламжлалт цэргийн хүчийг дангаар нь нэмэгдүүлэх замаар бус, харин технологийн инновац, кибер хамгаалалт, өндөр боловсролтой хүний нөөц, үндэсний тэсвэрлэх чадвар, үр ашигтай нөөц хүчний тогтолцоонд тулгуурлан хөгжүүлж байна. Үүний зэрэгцээ хиймэл оюун, өгөгдлийн боловсруулалт, сүлжээ төвт команд удирдлага, нисгэгчгүй систем зэрэг дэвшилтэт технологи нь орчин үеийн батлан хамгаалах чадавхын үндсэн бүрэлдэхүүн болж, батлан хамгаалах байгууллагуудын бүтэц, төлөвлөлт, сургалтын тогтолцоонд гүнзгий өөрчлөлт авчирч байна.

Судалгаанд хамрагдсан улс орнуудын нийтлэг туршлагаас харахад батлан хамгаалах боловсрол нь зөвхөн офицер бэлтгэх тогтолцоо бус, үндэсний инновац,

судалгаа, технологийн хөгжлийг дэмжих стратегийн төв болон хувьсан өөрчлөгдөж байна. Иймээс Монгол Улсын хувьд Эстоны кибер хамгаалалтын туршлага, Финландын бүх нийтийн аюулгүй байдлын үзэл баримтлал, Израилийн батлан хамгаалах инновацын экосистем зэрэг шилдэг туршлагыг үндэсний нөхцөлд нийцүүлэн хослуулан хэрэгжүүлэх нь ухаалаг батлан хамгаалах тогтолцоог хөгжүүлэх бодлогын хамгийн бодитой бөгөөд үр ашигтай хувилбар гэж үзэж болно. Мөн өгөгдөлд суурилсан команд удирдлага, хиймэл оюуны хэрэглээ, шинжлэх ухаан, инженерчлэл, мэдээллийн технологи, математикийн (ШИМТ/STEM) чиглэлийн боловсролыг батлан хамгаалах сургалтын тогтолцоонд үе шаттайгаар нэвтрүүлэх нь зүйтэй.

БАТЛАН ХАМГААЛАХ БОЛОВСРОЛЫН ШИНЭЧЛЭЛИЙН ХЭРЭГЦЭЭ БА ХӨГЖЛИЙН ЧИГ ХАНДЛАГА

Ухаалаг батлан хамгаалалтын эрин үе дэх цэргийн боловсролын шинэчлэл

Орчин үеийн батлан хамгаалах салбарын хөгжил нь зөвхөн шинэ зэвсэг, техник нэвтрүүлэх асуудлаар хязгаарлагдахгүй бөгөөд боловсрол, судалгаа, инновац, мэдээллийн чадавхыг хөгжүүлэхтэй салшгүй холбоотой болж байна. Зэвсэгт хүчний үр нөлөө нь хүний нөөцийн тоо хэмжээ, техник хэрэгслийн хүчин чадлаас гадна мэдээлэл боловсруулах чадвар, технологийн мэдлэг, шийдвэр гаргах хурд, инновацыг ашиглах чадамжаар улам бүр тодорхойлогдох болсон. Иймээс уламжлалт офицер бэлтгэх тогтолцоог шинэчлэн хиймэл оюун, кибер аюулгүй байдал, том өгөгдлийн шинжилгээ, нээлттэй эх сурвалжийн тагнуул (OSINT), танин мэдэхүйн дайн, дрон болон автономит систем, стратегийн харилцаа холбоо, дижитал команд удирдлагын чиглэлээр мэдлэг, ур чадвар эзэмшүүлэх шаардлага дэлхийн тэргүүлэх цэргийн их сургуулиудын нийтлэг чиг хандлага болж байна (NATO 2025).

Ухаалаг батлан хамгаалалтын эрин үеийн офицер нь зөвхөн командлагч бус, мэдээлэл боловсруулагч, технологийн хэрэглэгч, стратегич, судлаач байх шаардлагатай. Иймээс ирээдүйн офицер хиймэл оюун болон дижитал системийг ашиглах, их хэмжээний өгөгдөлд шинжилгээ хийх, OSINT мэдээллийг үнэлэх, кибер эрсдэлийг ойлгох, богино хугацаанд эрсдэлийг тооцоолон оновчтой шийдвэр гаргах, мөн геополитик, үндэсний аюулгүй байдал, технологийн хөгжлийн чиг хандлагыг стратегийн түвшинд цогцоор нь үнэлэх мэдлэг, ур чадвартай байх шаардлагатай.

Үндэсний батлан хамгаалахын их сургуулийн хөгжлийн шинэ чиглэл

Ухаалаг батлан хамгаалалтын тогтолцоог хөгжүүлэхэд Үндэсний батлан хамгаалахын их сургууль нь офицер бэлтгэх сургалтын байгууллагаас үндэсний хэмжээний батлан хамгаалах судалгаа, инновац, стратегийн шинжилгээний төв болон хөгжих шаардлагатай. Энэ хүрээнд цэргийн хиймэл оюун, кибер аюулгүй байдал, дрон ба автономит систем, цэргийн өгөгдлийн шинжлэх ухаан, OSINT, танин мэдэхүйн дайн, стратегийн харилцаа холбоо, батлан хамгаалах инновацын менежмент зэрэг шинэ чиглэлийг сургалт, судалгаанд үе шаттайгаар нэвтрүүлэх нь НАТО болон технологийн хөгжил өндөртэй орнуудын батлан хамгаалах боловсролын хөгжлийн чиг хандлагатай нийцэж байна (Lindley-French 2014).

Үүний зэрэгцээ симуляцад суурилсан сургалтын тогтолцоог хөгжүүлэх нь сургалтын чанар, үр ашгийг нэмэгдүүлэх стратегийн ач холбогдолтой. Виртуал бодит орчин (VR), нэмэгдүүлсэн бодит орчин (AR), кибер сургалтын талбар (Cyber Range), тактикийн симуляц, дижитал байлдааны орчин, хиймэл оюунд суурилсан байлдааны загварчлал зэрэг технологийг сургалтад ашигласнаар бодит техник хэрэгслийн хэрэглээг бууруулж, офицеруудын шийдвэр гаргах, нөхцөл байдлыг үнэлэх чадварыг илүү үр ашигтай хөгжүүлэх боломжтой. Иймээс ҮБХИС-ийн дэргэд Батлан хамгаалахын хиймэл оюуны лаборатори, Кибер симуляцын төв, Дроны сургалтын төв, Дижитал байлдааны лаборатори зэрэг төрөлжсөн судалгаа, сургалтын төвүүдийг үе шаттайгаар байгуулах шаардлагатай.

Батлан хамгаалах инновацын экосистем

Олон улсын туршлагаас харахад батлан хамгаалах шинэ технологийн хөгжил нь их сургууль, судалгааны байгууллага, хувийн хэвшил, төрийн байгууллагын нягт хамтын ажиллагаанд тулгуурладаг (R.V. Hasyn 2024). Монгол Улсын хувьд Батлан хамгаалах яам, Үндэсний батлан хамгаалахын их сургууль, судалгааны хүрээлэн, технологийн компаниуд болон Зэвсэгт хүчний хамтын ажиллагаанд суурилсан батлан хамгаалах инновацын экосистемийг бүрдүүлснээр дотоодын технологийн хөгжил, шинжлэх ухааны судалгаа, залуу судлаачдын оролцоог дэмжих, улмаар ухаалаг батлан хамгаалалтын тогтолцоог урт хугацаанд тогтвортой хөгжүүлэх боломж бүрдэх юм.

БАТЛАН ХАМГААЛАХ БОЛОВСРОЛЫН ШИНЭЧЛЭЛ БА УХААЛАГ БАТЛАН ХАМГААЛАЛТЫН ХӨГЖЛИЙН ЗАГВАР

Судалгааны үр дүнд Монгол Улсын нөхцөлд нийцсэн ”Ухаалаг батлан хамгаалах боловсролын загвар” болон “Ухаалаг батлан хамгаалах хөгжлийн загвар”-ыг санал болгож байгаа бөгөөд энэхүү загваруудын үндсэн зорилго нь батлан хамгаалах бодлого, боловсрол, судалгаа, инновац, технологи, хүний нөөцийн хөгжлийг нэгтгэсэн тогтолцоог бүрдүүлж, ухаалаг батлан хамгаалалтын шаардлагад нийцсэн шинэ үеийн офицер, судлаач, удирдагчдыг бэлтгэхэд оршино.

Энэхүү хандлагын хүрээнд Үндэсний батлан хамгаалахын их сургууль нь уламжлалт офицер бэлтгэх сургалтын байгууллагаас үндэсний хэмжээний батлан хамгаалах судалгаа, инновацын төв болон хөгжих шаардлагатай. Үүний тулд хиймэл оюун, кибер аюулгүй байдал, дрон ба автономит систем, өгөгдлийн шинжилгээ, танин мэдэхүйн дайн зэрэг чиглэлээр төрөлжсөн лаборатори, судалгааны төвүүдийг үе шаттайгаар байгуулж, Батлан хамгаалах яам, Зэвсэгт хүчин, эрдэм шинжилгээний байгууллага, хувийн хэвшлийн хамтын ажиллагааг бэхжүүлэх нь чухал юм.

Монгол Улсын хувьд ухаалаг батлан хамгаалалтыг хөгжүүлэхдээ өндөр өртөгтэй зэвсэглэл худалдан авахад төвлөрөхөөс илүүтэйгээр кибер хамгаалалт, хиймэл оюун, нисгэгчгүй систем, мэдээллийн аюулгүй байдал, өгөгдөлд суурилсан команд удирдлага, хүний нөөцийн хөгжилд үе шаттай хөрөнгө оруулалт хийх нь илүү оновчтой хөгжлийн чиглэл гэж үзэж байна. Ийм бодлого нь хязгаарлагдмал төсөвтэй нөхцөлд технологи, мэдлэг, инновац, олон улсын хамтын ажиллагаанд тулгуурлан батлан хамгаалах чадавхыг тогтвортой нэмэгдүүлэх боломжийг бүрдүүлнэ.

Үүнтэй уялдан Монгол Улсын ухаалаг батлан хамгаалалтын хөгжлийг дөрвөн үе шаттайгаар хэрэгжүүлэх боломжтой. **Эхний шатанд** эрх зүй, хүний нөөц, сургалтын тогтолцооны суурийг бүрдүүлж, **хоёрдугаар шатанд** кибер симуляц, хиймэл оюун, дрон технологийн туршилтын лабораториудыг байгуулан үндэсний нөхцөлд тохируулсан туршилт, нутагшуулалтыг хэрэгжүүлэх шаардлагатай. **Гуравдугаар шатанд** эдгээр технологийг команд удирдлага, сургалт, төлөвлөлтийн үйл ажиллагаатай уялдуулан нэгдсэн мэдээллийн орчин бүрдүүлж, эцсийн шатанд батлан хамгаалах бодлого, боловсрол, шинжлэх ухаан, технологи, үйлдвэрлэл хоорондын уялдаа холбоонд суурилсан үндэсний хэмжээний ухаалаг батлан хамгаалах тогтолцоог төлөвшүүлэх нь зүйтэй.

Ийнхүү ухаалаг батлан хамгаалалтын хөгжил нь зөвхөн шинэ техник, технологи нэвтрүүлэх асуудал бус, батлан хамгаалах боловсрол, судалгаа, инновац, хүний нөөцийн хөгжлийг нэгтгэсэн урт хугацааны стратегийн шинэчлэл болохыг энэхүү судалгаа харуулж байна. Энэ нь Монгол Улсын батлан хамгаалах чадавхыг эдийн засгийн боломжид нийцүүлэн тогтвортой бэхжүүлэх бодлогын оновчтой хувилбар гэж үзэж болно.

БОДЛОГЫН ЗӨВЛӨМЖ

Судалгааны үр дүнд үндэслэн Монгол Улсад ухаалаг батлан хамгаалалтыг хөгжүүлэхэд дараах бодлогын чиглэлийг тэргүүлэх ач холбогдолтой гэж үзэж байна. Үүнд:

- Батлан хамгаалах салбарын дижитал шилжилтийн нэгдсэн бодлогыг боловсруулж, кибер хамгаалалт, хиймэл оюун, өгөгдлийн шинжилгээ, нисгэгчгүй системийг батлан хамгаалах төлөвлөлт, сургалт, ажиллагаанд үе шаттай нэвтрүүлэх;
- Үндэсний батлан хамгаалахын их сургуулийн дэргэд хиймэл оюун, кибер хамгаалалт, дрон технологийн судалгаа, сургалтын төрөлжсөн төвүүдийг байгуулж, батлан хамгаалах боловсролыг шинэчлэх;
- Батлан хамгаалах яам, ҮБХИС, БХЭШХ, хувийн хэвшлийн хамтын ажиллагаанд тулгуурласан батлан хамгаалах инновацын экосистемийг хөгжүүлэх; мөн Эстон, Финланд, Израилийн туршлагыг Монгол Улсын нөхцөлд нийцүүлэн үе шаттай нутагшуулах шаардлагатай байна.

Үүний зэрэгцээ энхийг дэмжих ажиллагааны туршлагыг дрон, кибер хамгаалалт, мэдээллийн шинжилгээний сургалттай уялдуулж, нээлттэй эхийн программ хангамж, бага өртөгтэй дрон, симуляцад суурилсан сургалтын технологи зэрэг зардал багатай боловч өндөр үр ашигтай шийдлүүдийг үе шаттай нэвтрүүлэх нь эдийн засгийн боломжид нийцсэн хөгжлийн бодлогын чухал чиглэл гэж үзэж байна.

ДҮГНЭЛТ

XXI зууны аюулгүй байдлын орчин нь геополитикийн өрсөлдөөн, кибер аюул занал, хиймэл оюун, мэдээллийн дайн, автономит системийн хөгжлөөр тодорхойлогдож, батлан хамгаалах бодлого, байгуулалтын уламжлалт хандлагыг шинэчлэх шаардлагыг бий болгож байна. Судалгааны үр дүнгээс үзэхэд ухаалаг батлан хамгаалалт нь батлан хамгаалах төсвийн үр ашигтай зарцуулалтаас гадна, боловсрол, технологи, инновац, хүний нөөц, мэдээллийн чадавхыг нэгтгэсэн

стратегийн хөгжлийн үзэл баримтлал болох нь тогтоогдлоо.

Олон улсын туршлагын харьцуулсан шинжилгээ нь орчин үеийн батлан хамгаалах чадавхын үндэс нь кибер хамгаалалт, хиймэл оюун, нисгэгчгүй систем, өгөгдөлд суурилсан команд удирдлага, өндөр боловсролтой хүний нөөц болохыг харуулж байна. Монгол Улсын хувьд газарзүйн байршил, хүн ам, эдийн засгийн нөөц боломжийн онцлогийг харгалзан өндөр өртөгтэй уламжлалт зэвсэглэлээс илүү мэдлэг, технологи, инновацад тулгуурласан хөгжлийн бодлого илүү оновчтой болох нь энэхүү судалгаагаар нотлогдлоо.

Энэхүү судалгааны гол шинэлэг үр дүн нь Монгол Улсын нөхцөлд нийцсэн “**Ухаалаг батлан хамгаалах боловсролын загвар**” болон “**Ухаалаг батлан хамгаалах хөгжлийн загвар**”-ыг боловсруулан санал болгосонд оршино. Энэхүү загвар нь батлан хамгаалах боловсрол, судалгаа, инновац, технологи, хүний нөөцийн хөгжлийг нэгдсэн тогтолцоонд авч үзэх замаар ухаалаг батлан хамгаалалтын хэрэгжилтийн институцийн үндсийг тодорхойлж байна.

Иймээс Монгол Улсад ухаалаг батлан хамгаалах салбарыг хөгжүүлэх асуудал нь зөвхөн цэргийн шинэчлэлийн хүрээнд бус, боловсрол, шинжлэх ухаан, технологи, үндэсний инновац, төр-хувийн хэвшлийн хамтын ажиллагааг хамарсан урт хугацааны хөгжлийн бодлогын салшгүй хэсэг гэж үзэх нь зүйтэй. Цаашид энэхүү чиглэлээр онолын болон хэрэглээний судалгааг өргөжүүлэн хөгжүүлэх нь Монгол Улсын үндэсний аюулгүй байдал, батлан хамгаалах чадавхыг бэхжүүлэхэд чухал хувь нэмэр оруулах болно.

Эшлэл авсан сурвалж, судалгааны бүтээл:

1. Alvin Toffler, Heidi Toffler. 1994. *War and Anti-war: Survival at the Dawn of the 21st Century.* Warner Books.
2. Bisogniero, Claudio. 2011. “Speech on NATO’s Smart Defence Initiative.” *NATO’s Smart Defence Initiative.* Tallinn: NATO. 1.
3. Clausewitz, Carl von. 1984. *On War.* Princeton University Press .
4. Committee Security. 2023. *Security Strategy for Society.* Publication of the Finnish Government.
5. Creveld, Martin L. Van. 1991. *The Transformation of War.* Free Press.
6. Czosseck, Christian. 2011. “Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security.” *International Journal of Cyber Warfare and Terrorism.*
7. Henry A Kissinger, Eric Schmidt, Daniel Huttenlocher. 2021. *The Age of AI: And Our Human Future.* Little, Brown and Company.
8. Lindley-French, Julian. 2014. “Connected Forces Through Connected Education.”
9. NATO. Cooperative Cyber Defense Centre of Excellence. 2023. Annual Report, Tallinn.
10. NATO. 2025. “Defence Education Enhancement Programme (DEEP).” Brussels.
11. NATO. 2022. *Madrid Summit Declaration.* Official Text, Madrid : NATO.
12. R.V. Hasyn, O.Ia. Ivasechko, M.V. Zdoroveha. 2024. “Nato’s Innovative Projects In The Field Of Defense: The Defense Innovation Accelerator For The North Atlantic (Diana) And The Innovation Fund (Nif).” *Scientific Journal Regional Studies.*

13. RAND Corporation. 2001. *Networks and Netwars.* Monograph Report , RAND Corporation.
14. Rid, Thomas. 2013. *Cyber War Will Not Take Place.* Oxford: Oxford University Press.
15. Singer, P. W. 2009. *Wired for War.* New York: Penguin Press.
16. U.S. Department of Defense. 2022. “National Defense Strategy of the United States of America.” Washington D.C.