The Mongolian Journal of Strategic Studies Volume 35 | No 98 | 2025
https://doi.org/10.65315/mjss.v35i98.4849 Article

Монгол Улсын онц чухал дэд бүтцийн кибер аюулгүй байдлыг сайжруулахад Израилийн туршлагыг ашиглах нь

Мөнхчулууны Номин
Үндэсний аюулгүй байдлын магистр (MA), гэрээт судлаач nnoommiinn@gmail.com
Монгол Улс, Улаанбаатар, Үндэсний аюулгүй байдлын зөвлөлийн Стратеги судалгааны хүрээлэн

Хураангуй

Мэдээллийн технологи (IT) болон үйл ажиллагааны технологийн (OT) системүүдийн нэгдэл нь хөгжиж буй улсуудын онц чухал дэд бүтцэд урьд өмнө байгаагүй кибер аюулгүй байдлын сорилтуудыг бий болгож байна. Энэхүү судалгааны хүрээнд эрчим хүч, усан хангамж, тээвэр, харилцаа холбоо, хүнд хөнгөн үйлдвэрлэл зэрэг салбарын IT/OT нэгдлээс үүсэж буй эмзэг байдлыг шинжилж, Монгол Улсын онц чухал дэд бүтцийн өнөөгийн байдалд шинжилгээ хийсэн болно. Мөн Израилийн кибер аюулгүй байдлын тогтолцоог харьцуулсан загвар болгон ашиглаж, улс орны кибер сөрөн тэсвэрлэх чадавхыг сайжруулах арга хэмжээг санал болгохыг зорив.

Судалгааны үр дүнгээс үзвэл Монгол Улс буй кибер аюул, заналхийллээс онц чухал дэд бүтцээ хамгаалахын тулд иж бүрэн үндэсний стратеги боловсруулах, мэргэшсэн ажиллах хүчний хөгжилд хөрөнгө оруулалт хийх, төрийн болон хувийн хэвшлийн найдвартай түншлэлийг бий болгох шаардлагатай байна.

Түлхүүр үг: *IT/OT нэгдэл, кибер аюулгүй байдал, SCADA, ICS*

Оршил

Онц чухал мэдээллийн систем болон дэд бүтэц нь улс орнуудын эдийн засаг, үйлчилгээний тасралтгүй байдлыг хангах үндсэн тулгуур юм. IT болон OT системүүдийн нэгдэл сүүлийн жилүүдэд эрчимжсэнээр төрийн үйлчилгээ, үйлдвэрлэл, эрчим хүч, тээвэр зэрэг салбарын үр ашиг нэмэгдэж байгаа ч кибер халдлагад өртөх магадлал өсөж, том хэмжээний доголдол үүсэх эрсдэл нэмэгдсээр байна.

Монгол Улс нь өргөн уудам нутагтай, хүн ам цөөвтөр, эх газраар хүрээлэгдсэн онцлогтой учир онц чухал дэд бүтцээ хамгаалахад олон сорилттой тулгардаг. Эдийн засгийн дийлэнх, экспортын 90 орчим хувийг бүрдүүлдэг уул уурхай, эрчим хүч, харилцаа холбоо, тээвэр зэрэг салбарын харилцан хамаарал маш нягт билээ. Аж үйлдвэрийн хяналтын системүүд сүлжээний холболтоор улам хүртээмжтэй болохын хэрээр халдлагын гадаргуу эрс нэмэгдэж, өмнө нь зөвхөн IT орчинд илэрдэг байсан кибер аюул, заналд өртөх эрсдэлийг бий болгож байна.

Нэг. IT/OT нэгдлийн кибер аюулгүй байдлын ойлголт

IT/OT нэгдэл гэдэг нь өгөгдлийг боловсруулах, удирдахад зориулагдсан мэдээллийн технологийн системийг биет төхөөрөмж, түүний үйл явцыг хянах, удирдах үйл ажиллагааны технологиудтай нэгтгэхийг хэлнэ. Түүхэн хөгжлийг авч үзвэл үйлдвэрлэлийн хяналт мэдээллийн SCADA системүүд, Тархсан Хяналтын Системүүд DCS (Distributed Control Systems), PLC (Programmable Logic Controllers) зэрэг түгээмэл OT систем нь сүлжээнээс тусгаарлагдмал, “air gapping” байдлаар битүүмжлэлтэй ажиллан өөрсдийн аюулгүй байдлыг хангаж иржээ[1].

Аж үйлдвэржилтийн шинэ эринд үйл ажиллагааны үр ашгийг нэмэгдүүлэх, алсын зайн хяналтын чадварыг сайжруулах, засвар үйлчилгээг урьдчилан таамаглах эрэлт хэрэгцээ нэмэгдэхийн хэрээр аж үйлдвэрийн системүүдийг сүлжээ болон интернэтэд холбох шаардлага тулгарсан. Энэхүү нэгдэл нь бодит цагийн өгөгдлийн шинжилгээ хийх, шийдвэр гаргалтыг сайжруулах, үйл ажиллагааны зардлыг бууруулах ашиг тусыг өгдөг. Үүнтэй зэрэгцэн хязгаарлалтын арга хэмжээний чадамжийг бууруулан аюулгүй байдлын цар хүрээг бүдэгрүүлж эхэлсэн.

Халдлага үйлдэгчид бодит төхөөрөмжтэй шууд харилцах эрх олж авснаар PLC/RTU программыг өөрчлөх, насос хавхлага гэх мэт эд ангид буруу команд өгөх, өгөгдлийн тогтмол хэмжээ буюу “setpoint”-уудыг өөрчлөх, ослын дохиолол хамгаалалтыг идэвхгүйжүүлэх, хуурамч мэдээлэл урсгах зэргээр инженерийн хараанд өртөлгүй хортой үйл ажиллагаа явуулах болсон. Ингэснээр өгөгдлийн аюулгүй байдлаас гадна биет төхөөрөмжийн эвдрэл гэмтэл, саатал учрах, байгаль орчны гамшиг, хүний амь нас, эрүүл мэндэд шууд заналхийлэх зэрэг сөрөг үр дагаврыг орон зайнаас үл хамааран учруулах боломжтой болжээ. Энэ төрлийн халдлагад хариу арга хэмжээ авах, нөхөн сэргээх үйл ажиллагаа нь цаг хугацаа, нөөц маш ихээр шаарддаг байна.

Хоёр. Монгол Улсын онц чухал дэд бүтцийн өнөөгийн байдал, олон улсын кейс

Эрчим хүчний салбарт: Монгол Улсын эрчим хүчний дэд бүтэц нь IT/OT нэгдлийг хурдацтай нэвтрүүлж байгаа юм. Улсын цахилгаан сүлжээ нь дотоодын хэрэгцээг хангахаас гадна томоохон уул уурхайн үйл ажиллагааг явуулах тулгуур болж байна. Нүүрсний цахилгаан станц, салхи болон нарны цахилгаан станц зэрэг сэргээгдэх эрчим хүчний үйлдвэрийг төрийн өмчит Эрчим хүчний зохицуулах хороо хянадаг. Салбарын сүлжээний удирдлагад SCADA систем, ухаалаг тоолуур болон автомат хяналтын систем ашиглагддаг.

Дэлхийд томд тооцогдох Оюу толгойн зэс-алтны уурхай нь үйл ажиллагаандаа IT болон OT бүрэлдэхүүн хэсгүүдийг нэгтгэсэн автоматжуулалтын боловсронгуй системүүдийг ашигладаг[2]. Таван толгойн нүүрсний орд нь бутлах, ангилах, тээвэрлэх,

[1] Shankar Shastry “Taxonomy of cyber attacks on SCADA systems”, October 2011 - https://www.researchgate.net/publication/254049910_Taxonomy_of_cyber_attacks_on_SCADA_systems

[2] Oyu Tolgoi ”Q3 2025 Performance results”, Nov 2025 - ot.mn/en/news/q3-2025-performance-result

ачих зэрэг логистикийн үйл ажиллагаандаа автоматжуулалтыг нэвтрүүлсэн, цаашид олборлолт, боловсруулалтын үе шатанд ч шилжилт хийх боломжтой. Эдгээр систем үйл ажиллагааны үр ашгийг сайжруулдаг ч кибер заналхийлэлд өртөх олон тооны эмзэг цэгийг бий болгодог. Халдлагын гадаргуу нь интернэт сүлжээнд холбогдсон бүхий л төрлийн удирдлагын систем, алсын зайн хандалтын боломж болон хөндлөнгийн хүчин зүйлийн нөлөөнд өргөжин тэлдэг. Олон улсад эрчим хүчний дэд бүтэц рүү чиглэсэн ransomware буюу барьцаалах төрлийн халдлагын тоо 2024 оны байдлаар өмнөх жилтэй харьцуулахад 80 хувиар нэмэгдсэн[3]. Үүний шалтгааныг эрчим хүчний дэд бүтцэд тусгайлсан кибер аюулгүй байдлын иж бүрэн стандарт байхгүй, түүнчлэн уламжлалт "patch-and-update" арга барил нь үйл ажиллагааны тасралтгүй байдлыг хангахад төдийлөн тохиромжгүй байгаатай холбон тайлбарлаж байна.

Ус хангамж, ариутгах татуургын системд: Монгол Улсын хүн амын тавь орчим хувь нь Улаанбаатар хотод суурьшдаг ба хотжилт, уур амьсгалын өөрчлөлтийн нөлөөгөөр усан хангамжийн асуудалтай тулгарч байна. Хотын ус цэвэршүүлэх байгууламж, түгээлтийн сүлжээ, бохир болон саарал усны байгууламжууд нь бүгд удирдлагын нэгдсэн систем, алсын зайн хяналт, өгөгдлийн шинжилгээний автомат бүтцүүдийг ашигладаг[4]. Эдгээр нь нөөцийн удирдлагыг сайжруулан, гоожилт болон усны найрлагын чанарыг хянах, түгээлтийн оновчлолын боломжуудыг авчирна. Нөгөө талаас, усны бохирдол, түгээлтийн саатал, тасалдал, байгаль орчныг сүйтгэх зэрэг сөрөг асуудлыг дагуулдаг.

Энэ салбарт чиглэсэн кибер халдлагын онцлох жишээ бол 2021 оны хоёрдугаар сард АНУ-ын Флорида мужид нэгэн хакер ус цэвэршүүлэх байгууламжийн системд алсаас нэвтэрсэн явдал юм[5]. Гэмт этгээд Натрийн гидроксид (шүлт)-ийн хэмжээг 100 ppm-ээс 11,100 ppm хүртэл аюултай хэмжээнд нэмэгдүүлэхийг оролдсон нь тус мужийн 15000 оршин суугчийг хордуулах оролдлого байв. Халдагч нь хамгийн түгээмэл Windows 7 программ болон алсын зайн хандалтыг зөвшөөрдөг Team Viewer зэргийг ашиглажээ. Уг халдлагыг операторын сэрэмжтэй ажиллагааны ачаар сэргийлж чадсан.

Дэлхийд түгээмэл уг халдлагад өртөх магадлалтай олон усны байгууламжид тусгайлсан кибер аюулгүй байдлын хүний нөөц байхгүй бөгөөд аж үйлдвэрийн хяналтын системийн онцлогийг ойлгохгүй, ерөнхий IT мэргэжилтнүүдэд найдаж байгаа нь санаа зовоосон асуудал болоод байна.

Тээврийн салбарт: Монгол Улс нь тээврийн салбартаа мэдэгдэхүйц шинэчлэл хийж байгаа нь хэд хэдэн чиглэлээр илэрхий байна. Тухайлбал: Орос-Хятадыг холбосон Транс-Монголын төмөр замын удирдлага илүү боловсронгуй дохио, замын удирдлагын менежментийг ашигладаг болсон. "Чингис Хаан" олон улсын нисэх онгоцны буудал нь нислэгийн хөдөлгөөн, агаарын замын хяналт, ачаа тээшний үйл

[3] TrustWave Risk Radar Report /2025/ Energy and Utilities Sector - https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/2025_Trustwave_Energy_Utilities_Risk_Radar_Report.pdf

[4] УСУГ-ын албан ёсны цахим хуудас -Ус сувгийн удирдах газар

[5] ASDA - "Compromise of US Water Treatment Facility", Feb 2021 - Compromise of U.S. Water Treatment Facility | CISA

ажиллагаа, аюулгүй байдлын шалгалт болон байгууламжуудын удирдлагад нэгдсэн сүлжээг ашигладаг.

Улаанбаатар хотын зам тээврийн салбар мөн замын хөдөлгөөний гэрлийн зохицуулалт, тээврийн хэрэгслийн хяналт, шимтгэл авах автомат гарц зэрэгт ухаалаг систем нэвтрүүлэн, хиймэл оюун (ХО)-ы элементүүдийг ашиглаж[6] байгаа. Цаашид мөн хүнд оврын ачааны машины жолоочийн ухаалаг такограф системийг нэвтрүүлэх төлөвтэй. Эдгээр систем нь мэдрэгч, камер, холбооны сүлжээ, хяналтын системийн цогц бөгөөд замын хөдөлгөөний эмх замбараагүй байдал, осол эсвэл үйлчилгээний тасалдал үүсгэх аюултай кибер халдлагын бай болох эрсдэлтэй байна.

Харилцаа холбооны салбарт: Монгол Улсын харилцаа, холбооны салбар хурдацтай өсөж байгаа бөгөөд гар утасны нэвтрэлт 130 хувиас давж, 4G сүлжээ өргөжиж, 5G нэвтрүүлэн, сүлжээний цар хүрээг 2027 он гэхэд хүн амын 70 хувьд хүргэх зорилт[7] тавьсан байна. Гар утасны гурван томоохон оператор болон интернэт үйлчилгээ үзүүлэгчид бусад салбартай маш нягт уялдаатай ажилладаг. Уг салбар нь чухал дэд бүтцийн нэг хэсэг бөгөөд эрчим хүч, эрүүл мэнд, эдийн засаг, Засгийн газрын тасалдалгүй үйл ажиллагааг хангаж ажилладаг. Энэ салбарт DOS, SIM халдлага, луйвар залилан, тагнуулын үйл ажиллагаа тогтмол үйлдэгддэг. Хамгийн сүүлийн үеийн байдлаар 2025 оны тавдугаар сард DDOS халдлагын түүхэн хамгийн дээд хүчин чадалтай халдлагыг Aisuru botnet үйлдэж, секундэд 7.3 терабитээр 45 секунд буюу нийт 37.4 терабит траффик үүсгэсэн нь нэг дор 10 мянган өндөр чанартай кино ачаалсантай тэнцэхээр хэмжээнд хүрчээ[8]. Энэ төрлийн халдлагыг хорлон сүйтгэх, барьцаалах, улс төрийн гэх мэт зорилгоор түгээмэл үйлддэг.

Уул уурхай болон аж үйлдвэрийн салбарт: Уул уурхайн үйл ажиллагаа бол Монгол Улсын эдийн засгийн амин судас бөгөөд IT/OT нэгдлийг эрчимтэй нэмэгдүүлсэн. Орчин үеийн уурхайнууд автомат ачааны машинууд, алсын удирдлагатай өрмийн тоног төхөөрөмж, хүдрийн автомат боловсруулалт, нэгдсэн аюулгүй байдлын систем зэргийг өргөн ашиглаж байна. Эдгээр нь оновчлол, засвар үйлчилгээ, тасралтгүй үйл ажиллагаа зэргийг сайжруулахад шинжилгээ хийдэг асар их өгөгдлийн урсгалыг үүсгэдэг.

Харин энэ салбарын кибер халдлагууд барьцаалах, үйлдвэрлэлийн үйл ажиллагааг зогсоох, уул уурхайн том оврын тоног төхөөрөмжийн удирдлагыг алдагдуулах, тэсэлгээний бодис төхөөрөмжинд нөлөөлөх зэргээр үйлдэгддэг. Үр дүнд нь үйл ажиллагааны доголдол үүсэх, тоног төхөөрөмжийн гэмтэл учирч хөдөлмөрийн аюулгүй байдал алдагдах, геологи болон ашигт малтмалын нууц мэдээллийг алдах зэрэг маш их хэмжээний санхүү болон нөөцийн алдагдалд хүрдэг. Уг салбарт халдлагад өртсөн байгууллагууд ундажаар 2,540,000 ам.долларыг барьцаанд орсон

[6] The European - “British firm Skyral to help Mongolia tackle pollution with AI traffic modelling” July 2025 - AI Traffic Modelling Mongolia: How Skyral Is Helping Cut Pollution and Congestion

[7] Inside Mongolia, May 2025- Mongolia launches 5G Nationwide

[8] Cloudflare - “2025 Q3 report”, Dec 2025 - Cloudflare’s 2025 Q3 DDoS threat report -- including Aisuru, the apex of botnets

мэдээллээ олж авахад зарцуулдаг талаар Sophos-ийн судалгаанд дурдсан байна[9].

Гурав. Монгол Улсын кибер аюулгүй байдлын өнөөгийн байдал

Аюул, занал учруулагч, тэдний сэдэл: Монгол Улс нь бусад улсын адил өдөр тутамдаа гадаад болон дотоод хүчин зүйлийн нөлөөгөөр төрөл бүрийн кибер аюул, заналтай тулгардаг. Баримт дурдахад ЦХИХХЯ-ы мэдээлснээр ОХУ-аас 2024 оны байдлаар түүхэн дээд хэмжээ буюу 128 сая, БНХАУ-аас 50 сая, АНУ-аас 65 сая гаруй удаагийн сэжигтэй хандалт үйлдэгдсэн байна[10]. Гадаад хүчин зүйлийн хувьд хөрш орнуудын төрөөс ивээн тэтгэсэн халдлага үйлдэгчид уул уурхайн үйл ажиллагаа, дэд бүтцийн эмзэг байдал үүсгэх оролдлого хийх боломжтой[11].

Монгол Улсын хэмжээнд онц чухал мэдээллийн дэд бүтэцтэй 216 байгууллага байдагт эрүүл мэндийн байгууллага, банк, харилцаа холбоо, мэдээллийн технологийн үйлчилгээ эрхлэгчид, хилийн боомтын хяналт, удирдлагын систем болон улсын хилээр нэвтэрч байгаа зорчигч, тээврийн хэрэгслийн бүртгэл, мэдээлэл хариуцсан байгууллага, стратегийн ач холбогдол бүхий ашигт малтмалын ордыг ашиглах үйл ажиллагаа эрхлэгч зэрэг багтдаг байна.

Маш олон кибер гэмт хэргийн бүлэглэл чухал дэд бүтцийг санхүүгийн сэдлээр онилдог. АНУ-ын “Colonial Pipeline”-ийн ослоос харахад хортой программ нь үйл ажиллагааг албадан зогсоож, маш их хэмжээний мөнгөн төлбөрийг нэхэж, цаашдын үйл ажиллагаа, эргэн сэргэх нөхцөлийг улам дордуулсан. Монгол Улсын уул уурхайн үйл ажиллагаа өндөр үнэ цэнтэй ба үйлдвэрлэл, нөөцийн хувьд дэлхийд тэргүүлдэг учир эрсдэл ихтэй. Түүнчлэн Хактивист бүлгүүд нь улс төрийн эсвэл байгаль орчин, үзэл санааны шалтгаанаар халдлага их үйлддэг. Мөн дотоодоос шалтгаалсан, тухайлбал хүний нөөцийн асуудлаас үүдэлтэй ажилчдын сэтгэл санаа, ашиг сонирхол, боловсролын байдал зэрэг нь эмзэг байдлыг нэмэгдүүлэх хандлагатай байна.

Зохицуулалт болон эрх зүйн орчин: Монгол Улсын КАБ-ын хууль, эрх зүйн зохицуулалтын хүрээ нь хурдацтай сайжирсан ч учирч болох аюул, заналыг даван туулах чадавх хараахан бүрдээгүй. Мэдээллийн аюулгүй байдал өгөгдлийн хамгаалалт дээр харьцангуй дэвшилттэй байгаа ч чухал дэд бүтцийн КАБ-ыг тусгайлан иж бүрнээр зохицуулж чадахгүй байна. Өөрөөр хэлбэл: АНУ-ын NIST болон Европын Холбооны NIS2 заалттай адилтгах дэд бүтцийн операторуудад тодорхой стандартыг өгдөг дүрэм журам байхгүй байна.

Дөрөв. Израилийн чухал дэд бүтцийн КАБ-ын талаар

Үндэсний КАБ-ын бүтэц: Израил нь чухал дэд бүтцийн КАБ-ын хувьд дэлхийн хамгийн боловсронгуй бүтцийг хөгжүүлсэн. Энэ нь аюулгүй байдал болон мэдээллийн технологийн чадавхаар давхар бэхэжсэн байдаг. Анх 2017 онд байгуулагдсан

[9] Sophos “The State of Ransomware in Critical Infrastructure 2024” - https://assets.sophos.com/X24WTUEQ/at/75tnw-38cqsnrrv56wpwc78k/sophos-state-of-ransomware-critical-infrastructure-2024.pdf

[10] UBPOST ”Sponsored hackers threaten government’s security” /2025.11.28/ -_https://www.ubpost.mn/a/13656

[11] Global Cyber Security Capacity Centre “Cybersecurity capacity review Mongolia”, 2025 - mongolia_cmm.pdf

Израилийн Үндэсний Кибер Удирдлага (INCD) нь орон даяар КАБ-ын эрх мэдлийг хэрэгжүүлэгч төвлөрсөн удирдлагаар хангадаг байгууллага юм. Засгийн газрын олон яам агентлаг, онц чухал дэд бүтцийн операторууд, төр хувийн хэвшлийн уялдаа холбоог хангаж, чиг үүрэг өгч, стратегийн чиглэл зорилтыг баталж, зохицуулалтыг хянаж түүнчлэн үйл ажиллагаанд нь дэмжлэг өгч ажилладаг.

Дээрх үйл ажиллагааны хүрээнд хэд хэдэн гол зарчмыг онцолдог. Үүнд:

Нэгдүгээрт, кибер аюулгүй байдалд Засгийн газраас өндөр түвшинд анхаарч, үндэсний аюулгүй байдлын тэргүүлэх чиглэл гэж хүлээн зөвшөөрдөг.

Хоёрдугаарт, онц чухал дэд бүтцийн салбарууд үйл ажиллагаандаа тусгай аюулгүй байдлын шаардлагыг заавал биелүүлэх нөхцөлтэйгөөр мөрддөг.

Гуравдугаарт, онц чухал дэд бүтцийн ихэнх хэсэг нь хувийн өмчид байгааг хүлээн зөвшөөрч, төрийн болон хувийн хэвшлийн өргөн хүрээний түншлэлийг дэмждэг.

Дөрөвдүгээрт, цэргийн болон төрийн алба хаагчдыг чиг үүргийн хүрээнд мэдлэг олгож ажиллах хүч болгон дайчилдаг.

Зохицуулалт болон стандартууд: Израилийн онц чухал дэд бүтцийн хамгаалалт хэд хэдэн түвшний зохицуулалт дээр суурилдаг. Нэн тэргүүнд INCD-ээс онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудыг үйл ажиллагааны цар хүрээ, ач холбогдлын үндсэн дээр ангилж, эрэмбэ тогтоон, түүнд тохирох аюулгүй байдлын стандартуудыг баталсан. Жишээлбэл: Нэгдүгээр түвшний байгууллагууд, тэдгээрийн үйл ажиллагааны тасалдал нь үндэстэнд хамгийн их хор хохирол учруулах боломжтой гэж үзэж хамгийн хатуу зохицуулалтыг хэрэгжүүлдэг.

Эдгээр нь заавал мөрдөх хяналтын арга хэмжээ, эрсдэлийн үнэлгээний журам, осол тайлагнах үүрэг, тогтмол сайжруулалт зэргийг багтаасан байдаг. Хэрэгжүүлээгүй тохиолдолд торгууль болон үйл ажиллагааны хязгаарлалт зэрэг албадлагын арга хэмжээг авдаг. Дан хориг, санкцаар шахах бус аюулгүй байдлын шаардлагыг үйл ажиллагааны бодит байдалтай тэнцвэржүүлэн, байгууллагуудад үүргээ биелүүлэхэд нь туслах техникийн удирдамж, хэрэгсэл тоног төхөөрөмжийн хангамж зэрэг дэмжлэгийг үзүүлдэг нь маш сайн жишиг гэж үзэж байна. Цаашилбал:"Үндэсний КАБ-ын бэлэн байдлын баг[12]" нь чухал дэд бүтцүүдэд осол хариу арга хэмжээний туслалцаа, аюул, заналын мэдээлэл солилцоо, урьдчилсан эмзэг байдлын шинжилгээ зэрэг үйлчилгээг тогтмол үзүүлдэг.

Авьяас хөгжүүлэлт: Израилийн КАБ-ын чадавхын өндөр түвшин нь 8200[13] дугаар элит анги нь цэргийн албан хаагчдад КАБ, дохионы мэдээлэл, мэдээллийн дайны өндөр түвшний сургалтыг тогтмол зохион байгуулдаг. Алба хаасны дараа олон залуус КАБ-ын салбарт орж, өөрийн компаниа байгуулж, эсвэл одоо амжилттай үйл ажиллагаа явуулж байгаа компаниудад ажилладаг.

[12] INCD "National CERT" - Computer Emergency Response Center (CERT) - Computer Emergency Response Center (CERT) for cyber incident handling – hotline 119 Israel National Cyber Directorate

[13] Cyber 8200 "OSINT handbook", Jul 2025 -

Энэхүү цэргийн болон иргэний сүлжээ нь онцгой давуу тал болдог ба бодит туршлага болон төр-хувийн хэвшлийн хамтын ажиллагааг хөнгөвчилдөг байна. Түүнчлэн их, дээд сургуулиуд нь тусгайлсан кибер аюулгүй байдлын хөтөлбөрүүдийг санал болгож, Засгийн газар нь судалгаа, хөгжүүлэлтийн ажилд тэтгэлэг санхүүжилт олгох, хамтрал болон түншлэлийг дэмждэг.

Үүний үр дүнд инновацын экосистем нь Израилийг дэлхийн КАБ-ын төв болгоод зогсохгүй компаниуд олон улсын манлайлагчийн үүрэг гүйцэтгэж байна. Олон улсын түвшинд Израил хоёр талын гэрээ байгуулах, олон талт форумд оролцох, худалдааны харилцаагаар дамжуулан олон улсын КАБ-ын хамтын ажиллагаанд идэвхтэй оролцдог.

Дүгнэлт

Израилийн кибер аюулгүй байдлын загвар нь кибер аюулгүй байдлыг үндэсний аюулгүй байдлын тэргүүлэх чиглэл болгох, хууль эрх зүйн орчин бүрдүүлэх, цэргийн албан хаагчдад сургалт зохион байгуулах, хөрөнгө оруулах, төрийн болон хувийн хэвшлийн түншлэлийг дэмжих, олон улсын хамтын ажиллагааг үүсгэх зэрэг сайн туршлагыг нэвтрүүлсэн. Энэ хандлага нь Израилийг дэлхийн кибер аюулгүй байдлын манлайлагч болгон хөгжүүлсэн байна.

Ирээдүйн кибер аюулгүй байдлын талбар нь улам нарийн төвөгтэй болж байна. ХО болон машин сургалт нь кибер орчныг үсрэнгүй хөгжүүлэхийн зэрэгцээ давхар эрсдэл үүсгэж байна. Мөн 5G сүлжээ болон зүйлсийн интернэт нь холбогдсон төхөөрөмжүүдийг хэдэн арван тэрбум хүртэл нэмэгдүүлж, халдлагын гадаргууг өргөжүүлж байгаа. Квант тооцоолол нь одоогийн шифрлэлтийг эвдэх аюул учруулж, шинэ шифрлэлтийг дэлхий даяар эрэн хайсаар байна.

Монгол Улс нь эдгээр чиг хандлагыг урьдчилан таамаглаж, одооноос бэлтгэх ёстой. Энэ нь КАБ-ын хөгжилд хөрөнгө оруулалт хийх, олон улсын стандартууд болон сайн практикийг нутагшуулах, чадавхыг тасралтгүй шинэчлэх, уян хатан байх хандлагыг шаардаж байна. Кибер аюул, заналхийлэл нь хариу үйлдэлд тулгуурладаг учир бүх төрлийн нөхцөл байдалд урьдчилан бэлтгэлтэй байх хэрэгтэй. Онц чухал дэд бүтцийн эвдрэл нь эдийн засгийн хохирол, орчны гамшиг, амь насанд заналхийлэх, олон улсын итгэлийг алдах үр дагаврыг авчирдаг. Монгол Улс хүн амын бүтцийн хувьд залуучууд давамгайлсан, технологийн салбарын хурдацтай хөгжил, аналитик сэтгэлгээ болон инженерчлэлийн чадвар маш өндөр зэрэг өөрийн давуу талтай. Эдгээр давуу талыг ашиглаж, бусад улсын туршлагаас суралцаж, тодорхой бодлогыг хэрэгжүүлснээр чадварлаг кибер аюулгүй байдлын байр суурийг бий болгох боломжтой.

Санал, зөвлөмж

Израилийн дэд бүтцийн КАБ-ын амжилтын гол түлхүүр нь энэ асуудлыг үндэсний аюулгүй байдлын тэргүүлэх чиглэл болгон үзэж, төрийн дээд түвшинд тууштай

анхаарч, тасралтгүй хөрөнгө оруулалт хийсэнд оршино. Хэдийгээр Израилийн загварыг шууд хуулбарлах боломжгүй ч Монголын нөхцөл байдалд тохируулан дараах зарчмыг хэрэгжүүлэх боломжтой. Үүнд:

- ***Стратегийн түвшинд:*** Онц чухал дэд бүтцийн кибер аюулгүй байдлыг үндэсний аюулгүй байдлын асуудал гэж албан ёсоор хүлээн зөвшөөрөх, Засгийн газрын хэмжээнд салбар хоорондын зохицуулалт, тогтвортой хөрөнгө оруулалтын бодлого боловсруулж, зорилтоо тодорхойлох, хариуцах байгууллага түүний тогтолцоо, хэрэгжүүлэх хугацааны хуваарь, хэмжигдэхүйц үзүүлэлтүүдийг нарийвчлан тогтоох;
- ***Бүтцийн түвшинд:*** Израилийн INCD[14]-тэй адилтгаж одоо үйл ажиллагаа явуулж байгаа агентлагуудын хоорондын хамтын ажиллагааг зохицуулж, стандарт боловсруулж, шаардлагатай дэмжлэг үзүүлэх үндэсний төвлөрсөн байгууллага байгуулах. Энэ байгууллага нь чухал дэд бүтцийн ангиллын эрэмбийг тодорхойлох, заавал мөрдөх аюулгүй байдлын стандартыг тогтоож мөрдүүлэх, ослын мэдээллийг төвлөрүүлж, мэдээ, мэдлэг солилцох, стратегийн хэрэгжилтийг хангах, дэмжлэг үзүүлэх үүргийг гүйцэтгэх;
- ***Хүний нөөцийн хөгжүүлэлтэд:*** Их, дээд сургуулиудад кибер аюулгүй байдлын тусгайлсан хөтөлбөрүүдийг нэвтрүүлж, тэтгэлгээр залуусыг энэ салбарт татах нь ажиллах хүчний нөөц бүрдүүлэх, төр-хувийн хэвшлийн хамтын ажиллагааг бэхжүүлнэ, иргэн болон цэргийн алба хаагчдыг дайчлан мэргэжилтний хөрвөх чадварыг баталгаажуулах механизм бүрдүүлэх боломжийг судлах; Одоо байгаа IT суурьтай инженерийн хүний нөөцөд зориулан OT системүүдийн талаар дахин сургалт зохион байгуулах, мэргэшүүлэх сургалт, олон улсын гэрчилгээний хөтөлбөр, практик дадлага, симуляцийн орчинд ажиллах туршлага зэргийг багтаасан цогц хөтөлбөрийг Засгийн газар болон салбарын холбоод нь санхүүжүүлж, идэвхтэй дэмжих;
- ***Техникийн түвшинд:*** Сүлжээг сегментжүүлэх буюу IT/OT системүүдийн хоорондох уялдаа холбоо болон хязгаарыг тодорхойлох, халдлагын үед тархалтыг нэн даруй хязгаарлах, чухал дэд бүтцийн тасралтгүй ажиллагааг хангах шат дараалыг батлах; Хамгаалалтын галт хана, дотоод мэдрэгчийн систем (IDS/IPS), хандалтын хяналт, олон хүчин зүйлийн баталгаажуулалт (MFA) зэрэг олон улсад өргөн ашиглагддаг техникийн хамгаалалтын арга хэмжээг нэвтрүүлэх; Эмзэг байдлын үнэлгээ болон нэвтрэх туршилт (penetration test) тогтмол явуулах (дотоодын баг бүрэлдэхүүн эсвэл хөндлөнгийн мэргэжилтнүүдээр хийлгэж, үр дүнг эрэмбэлэн хариу арга хэмжээ авах); Ослын тохиолдлын үеэр авах хариу арга хэмжээний иж бүрэн төлөвлөгөө гаргаж, дэд бүтцийн удирдлага бүрийг мэдээллээр хангах (төлөвлөгөө нь олон төрлийн кибер осол, ransomware хортой программ, системийн үйл ажиллагаа, дотоодын эрсдэл зэргийг хамарсан байх ёстой ба тогтмол дадлага хийж туршин, үр дүнгийн дагуу шинэчлэлт хийгддэг байх);

[14] INCD Official page - Israel National Cyber Directorate

- ***Төсвийн болон Олон улсын туншлэлийн хүрээнд:*** Дэд бүтцийн КАБ-ын хөрөнгө оруулалтыг зарлага биш хөрөнгө оруулалт гэж харах жишгийг төрхувийн хэвшилд нэвтрүүлэх; Онц ухал дэд бүтцийн операторын КАБ-ын зардлыг үйл ажиллагааны зардлын салшгүй хэсэг болгон тооцох; Хууль эрх зүйн орчны зохицуулалт, татварын хөнгөлөлт, урамшууллын бодлогоор дэмжин идэвхжүүлэх; Олон улсын санхүүгийн байгууллагууд болох Дэлхийн банк, Азийн хөгжлийн банк[15], хоёр болон олон талт хөгжлийн түншүүд нь кибер аюулгүй байдлын төслүүдийг өргөн хүрээнд дэмждэг болсон тул эдгээр эх үүсвэрийг идэвхтэй ашиглах, олон улсын дэмжлэг авах боломжийг эрэлхийлэх зэрэг үйл ажиллагааг хэрэгжүүлэх боломжтой.

Эх сурвалжийн жагсаалт

Shankar Shastry “Taxonomy of cyber-attacks on SCADA systems”, October 2011 - https://www.researchgate.net/publication/254049910_Taxonomy_of_cyber_attacks_on_SCADA_systems.

Oyu Tolgoi ”Q3 2025 Performance results”, Nov 2025- ot.mn/en/news/q3-2025-performance-results?utm_source=chatgpt.com

TrustWave “Risk Radar Report /2025/ Energy and Utilities Sector” - https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/2025_Trustwave_Energy_Utilities_Risk_Radar_Report.pdf

УСУГ-ын албан ёсны вебсайт - Ус сувгийн удирдах газар

ACDA - Compromise of US Water Treatment Facility - Compromise of U.S. Water Treatment Facility | CISA

The European - “British firm Skyral to help Mongolia tackle pollution with AI traffic modelling”, July 2025 - AI Traffic Modelling Mongolia: How Skyral Is Helping Cut Pollution and Congestion

Inside Mongolia Mongolia launches 5G Nationwide

Cloudflare - “2025 Q3 report”, Dec 2025 - Cloudflare’s 2025 Q3 DDoS threat report -- including Aisuru, the apex of botnets

Sophos “The State of Ransomware in Critical Infrastructure 2024” - https://assets.sophos.com/X24WTUEQ/at/75tnw38cqsnrrv56wpwc78k/sophos-state-of-ransomware-critical-infrastructure-2024.pdf

UBPOST ”Sponsored hackers threaten government’s security” /2025.11.28/ - https://www.ubpost.mn/a/13656

Global Cyber Security Capacity Centre “Cybersecurity capacity review Mongolia”, 2025 - mongolia_cmm.pdf

INCD “National CERT” - Computer Emergency Response Center (CERT) for cyber incident handling – hotline 119 Israel National Cyber Directorate

[15] ADB ”Cybersecurity Multi-Donor Trust Fund“ - Cybersecurity Multi-Donor Trust Fund

Cyber 8200 “OSINT handbook”, Jul 2025 - Unit 8200: Expanded OSINT Handbook to Israel’s Cyber-Intelligence Powerhouse

INCD Official page - Israel National Cyber Directorate

ADB ”Cybersecurity Multi-Donor Trust Fund“ - Cybersecurity Multi-Donor Trust Fund

Enhancing Critical Infrastructure Cybersecurity in Mongolia Using Israel’s Experience

Nomin Munkhchuluun

Master of Arts in National Security, Non-resident researcher nnoommiinn@gmail.com
The Institute for Strategic Studies, National Security Counsil, Ulaanbaatar Mongolia

Abstract

The convergence of Information Technology (IT) and Operational Technology (OT) systems in critical infrastructure presents unprecedented cybersecurity challenges for developing nations. This research examines Mongolia’s evolving critical infrastructure landscape, analyzing the vulnerabilities emerging from IT/OT integration in sectors including energy, water management, transportation, heavy industries, and telecommunications. Drawing on Israel’s successful cybersecurity framework as a comparative model, this study identifies key gaps in Mongolia’s current approach and proposes actionable recommendations for enhancing national cybersecurity resilience.

The findings suggest that Mongolia must develop comprehensive national strategies, invest in specialized workforce development, and establish robust public-private partnerships to secure its critical infrastructure against increasingly sophisticated cyber threats.

Keywords: *IT/OT convergence, cybersecurity, SCADA systems, ICS*

Received: December 1, 2025 | Accepted: December 25, 2025 | Published online: December 30, 2025