КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ТАЛААР УЛС ОРНУУДЫН ХАМТЫН АЖИЛЛАГААНЫ ЧИГ ХАНДЛАГА: МОНГОЛ УЛС, ОХУ, БНХАУ-ЫН КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ХАМТЫН АЖИЛЛАГААНЫ ЭРХ ЗҮЙН ЗОХИЦУУЛАЛТ

ANALYZING THE POLICY COOPERATION ON CYBER SECURITY OF THE MONGOLIA BETWEEN RUSSIA AND CHINA

Л.Галбаатар
Монголын Хуульчдын холбооны гишүүн, хуульч

Товч агуулга: Монгол Улсын Үндэсний аюулгүй байдлын үзэл баримтлалд, Монгол Улс нь ОХУ, БНХАУ-тай сайн хөршийн найрсаг харилцаа, өргөн хүрээтэй хамтын ажиллагааг хөгжүүлэх, бүхэлдээ тэнцвэртэй харилцахыг эрмэлзэх талаар тусгасан. Гэвч мэдээллийн үсрэнгүй хөгжлийн эрин үед БНХАУ, ОХУ-ын нутаг дэвсгэрээс Монгол Улс уруу чиглэсэн кибер халдлага ихээхэн нэмэгдэх болсон. Иймд энэ өгүүллээр, аюулгүй байдал, түүний дотор мэдээллийн аюулгүй байдлыг хангах салбарт Монгол Улс, хөрш хоёр оронтой хоёр болон гурван талын харилцаа, хамтын ажиллагааг хөгжүүлэх эрх зүйн орчныг тодруулах замаар цаашид хөрш хоёр орон болон бусад улстай кибер аюулгүй байдлыг хангах асуудлаар харилцахад анхаарах асуудлыг дэвшүүлэв.

Abstract: Mongolia has declared in the National Security Concept that neighbor-friendly relations and a wide-ranging cooperation with the Russian Federation and the Peoples Republic of China shall be developed. Despite this, individuals and other groups both in China and Russia have attempted cyber-attacks numerous times and most of which have been recorded. It can be observed that our two neighbors do try to access information and databases in Mongolia surpassingly. This article examines the cooperation policy on the cyber security of Mongolia with Russia and China. Correspondingly, it sets out the key directions on ensuring the cyber security of Mongolia.

Түлхүүр үгс: *Хоёр хөрш, Кибер аюулгүй баадал, Хамтын ажиллагаа, Олон улсын эрх зой.*

Keywords: *Neighboring Countries; Cybersecurity; Cooperation; International Law*

Оршил

2016 оны 3 дугаар сарын байдлаар Монгол Улсын “интернетийн урсгал" дээр кибер халдлага үйлдсэн улс орнуудын дотроос манай хоёр хөрш буюу БНХАУ. ОХУ давамгайлах болсон нь ажиглагдлаа. Ер нь манайд ийм үйлдэл явуулж байгаа улс орны тоонд АНУ, Тайвань, БНСУ багтаж байгаа юм[1] .

Кибер халдлага нь, кибер гэмт хэргийн төрөл төдийгүй кибер аюулгүй байдалд заналхийлэх голлох эх үүсвэр юм. НҮБ-ын мэдээлснээр кибер халдлага нь үндэстэн дамнасан зохион байгуулалттай гэмт хэрэгт хамаарах бөгөөд дэлхийн эдийн засагт жил бүр нэг тэрбум америкийн долларын хохирол учруулж байгаа ноцтой үр дагавартай юм[3].

Ийм нөхцөлд Монгол Улсын зүгээс кибер аюулгүй байдлаа хангах, цахим орчинд бусад улс, этгээдтэй сөргөлдөх аюулаас сэргийлэх зорилгоор хөрш хоёр оронтойгоо хоёр болон гурван талын харилцаа, хамтын ажиллагааг хөгжүүлэхэд холбоотой эрх зүйн орчныг тодруулах, түүнийг шинжлэн судлах шаардлага нэгэнт үүсчээ[4].

Ингээд энэ өгүүллээр, Монгол Улс, ОХУ, БНХАУ гэсэн гурван орны кибер аюулгүй байдлыг хангах хамтын ажиллагааны эрх зүйн орчин болон өнөөгийн нөхцөл байдлыг дүгнэж танилцуулах, цаашид Монгол Улсаас хөрш хоёр оронтой кибер аюулгүй байдлыг хангах асуудлаар яаж тэнцвэртэй харилцах болон кибер аюулгүй байдлыг хангахад цаашид анхаарах асуудлын талаар үндсэн гурван хэсэг бүхий бүтцийн хүрээнд байр сууриа танилцуулж байна. Үүнд,

1. Үндэсний аюулгүй байдал ба цахим орчны харилцан хамаарал;
2. Монгол Улс, ОХУ, БНХАУ-ын цахим орчинд үндэсний аюулгүй байдлыг хангах бодлого, эрх зүйн зохицуулалт;
3. Кибер аюулгүй байдлыг хангах асуудлаар Монгол Улс, ОХУ, БНХАУ-ын өнөөгийн байдал, чиг хандлага тус тус багтаж байна.

Нэг. Үндэсний аюулгүй байдал ба цахим орчны харилцан хамаарал

[1] Кибер аюулгүй байдлын газар. Монгол Улсын интернетийн 0.02% урсгал дээр хийгдэж буй халдлагын шинж бүхий хандалт 2016 оны 2 дугаар сар. 2016.03 http://ncsc.gov.mn/?id=l 32

[2] Л.Галбаатар. Кибер гэмт хэргийг шүүхэд хянан шийдвэрлэх нь. МУИС Пресс хэвлэлийн газар.
Улаанбаатар. 2015. 13 дахь тал

[3] United Nations Office on Drugs and Crime. Transnational organized crime: the globalized illegal economy
https://www.unodc.org/toc/en/crimes/organized-crime.html

[4] Монгол Улсын Үндэсний аюулгүй байдлын үзэл баримтлал (2010)-ын 3.6.1.12-т Мэдээллийн аюулгүй байдлыг хангах, мэдээллийн орчинд сөргөлдөх аюулаас сэргийлэх, кибер орчин дахь гэмт явдалтай тэмцэх чиглэлд олон улсын хамтын ажиллагааг өргөжүүлэн хөгжүүлнэ гэж заасан.

1990-ээд оноос эхлэж, АНУ-ын тухайн үеийн ерөнхийлөгч Б.Клинтоны тамгын газраас, үндэсний аюулгүй байдал ба интернет хоорондын хамаарлыг дэвшүүлэн ярьсан байдаг[5].

Интернетийг зөвхөн нэг улс эзэмшихгүй бөгөөд түүнийг нийт байгууллага, иргэн ашиглах боломжтой болгохын хувьд улс орнууд интернетийг зөвхөн тухайн улсын нутаг дэвсгэртэй адил, дангаар эзэгнэн засаглах боломжгүй юм.

Үндэсний аюулгүй байдлын үзэл баримтлалын үүднээс, цахим орчинд тухайн улсын үндэсний язгуур ашиг сонирхлыг хангах гадаад, дотоод таатай нөхцөл бүрдсэн байхыг, тухайн улсын кибер аюулгүй байдал гэж үзэж болох юм[6].

Цахим орчин *(Cyberspace)* гэдэгт, юуг ойлгох талаар бүх нийтээр хүлээн зөвшөөрсөн тодорхойлолт байхгүй хэдий боловч интернет, харилцаа холбооны сүлжээ, компьютерын сүлжээ, процессор зэрэг мэдээллийн технологийн харилцан хамааралтай дэд бүтцийн сүлжээнээс бүрдэх дэлхий нийтийн мэдээллийн орчин дахь орон зай, гэж ойлгодог[7]. АНУ, БНХАУ, ОХУ, Израиль, Франц зэрэг олон улс орон, цахим орчин дахь зөрчил, мөргөлдөөнд бэлтгэж байна[8]. Тухайлбал, АНУ-ын хувьд “Цахим орчны олон улсын стратеги” хэмээх баримт бичгийг 2011 оны 5 дугаар сард хэрэгжүүлж эхлэсэн бөгөөд түүнд цахим орчин дахь аюулгүй байдлыг хангах үйл ажиллагааны голлох дөрвөн шинжийг тодорхойлсон байна. Үүнд,

- инновацид нээлттэй байх;
- хүмүүсийн итгэлийг олж авах буюу түүнийг алдахгүйн тулд аюулгүй байдлыг хангалттай хангах;
- дэлхий даяар харилцан хамтран ажиллах боломжтой байх;

[5] Derek S. Reveron. “An Introduction to National Security and Cyberspace”, pp. 3-20. Cyberspace and National Security: threats, opportunities, and power in a virtual world / Derek S. Reveron, editor. Georgetown University Press. Washington DC. 2012. p.6

[6] Монгол Улсын Үндэсний аюулгүй байдлын үзэл баримтлал (2010)-ын 1.1.1-т “Монгол Улсын үндэсний аюулгүй байдал гэж Монгол Улсын үндэсний язгуур ашиг сонирхлыг хангах гадаад, дотоод таатай нөхцөл бүрдсэн байхыг хэлнэ” гэснийг үндэслэн улс орны кибер аюулгүй байдлын тухай тохируулан тайлбарлав.

[7] “Cyber Space” буюу цахим орчин гэдэгт юуг ойлгох талаар улс орнууд янз бүрээр тайлбарласан байгааг эндээс үзэж болно.

Cyber Definitions. CCDOE. https://ccdcoe.org/cvber-definitions.html;

Tim Maurer & Robert Morgus. Compilation of Existing Cybersecurity and Information Security Related

Definitions. Report. 2014.10. p. 18 https://static.newamerica.org/attachments/175-compilation-of-existing-cvbersecuritv-and-information-securitv-related-definitions/OTI Compilation of Existing Cybersecurity and Information Security Related Definitions Updated 122015.pdf

[8] Derek S. Reveron. “An Introduction to National Security and Cyberspace”, pp. 3-20. Cyberspace and National Security: threats, opportunities, and power in a virtual world / Derek S. Reveron, editor. Georgetown University Press. Washington DC. 2012. p.4

- найдвартай байх[9].

Энд дурдсан аюул заналын эсрэг, найдвартай байдлыг хангах нь өнөөдөр үндэсний аюулгүй байдлыг хангахтай холбоотой яриа, хэлэлцүүлэгт давамгайлах болсон бөгөөд ирээдүйн аюул занал, дайны адил санаа зовоох зүйл болсон талаар судлаачид онцлох болов[10] [11].

Умард Атлантын Гэрээний Байгууллага (NATO)-ын Кибер довтолгооноос хамгаалах хамтын ажиллагааны төв (CCDCOE)-өөс түүвэрлэн бэлтгэсэн, улс орнуудын кибер аюулгүй байдлын бодлого, эрх зүйн баримт бичгийн жагсаалтаас харахад, өнөөдөр кибер аюулгүй байдлыг хангахад ихэнх улс орон онцгой анхаарч байгаа нь тодорхой байна". Тодруулбал, дараах улс орон кибер аюулгүй байдлын бодлого, эрх зүйн баримт бичиг боловсруулж, хэрэгжүүлж байна. Үүнд,

НАТО-гийн гишүүн орнууд:

Албани, АНУ, Бельги, Болгар, Дани, ИБУИНВУ, Исланд, Испани, Итали, Канад, Латви, Литва, Люксенбург, Нидерланд, Норвеги, Полып, Португали, Румын, Словак, Словени, Турк, Унгар, Франц, ХБНГУ, Хорват, Чех, Эстони.

НАТО-гийн гишүүн бус орнууд:

Европын бүс нутгаас: Австри, Босни-Герцеговин, Гүрж, Европын холбоо, Ирланд, Кипр, Монтенегро, ОХУ, Серби, Украин, Швед, Швейцар, Финланд.

Ази, Номхон далайн бүс нутгаас: Австрали, Азербайжан, Арабын нэгдсэн Эмират, Афганистан, Бангладеш, БНСУ, БНХАУ, Катар, Малайз, **Монгол,** Пакистан, Саудын Араб, Сингапур, Шинэ Зеланд, Энэтхэг, Япон,

Африкийн бүс нутгаас: Африкийн холбоо, Ботсвана, Гамби, Гана, Египет, Зимбабве, Кени, Маврикий, Мавритани, Марокко, Нигер, ӨАБНУ, Уганда.

Америк, Карибын тэнгисийн бүс нутгаас: Бразил, Гренада, Колумб, Коста Рика, Панам, Тринидад-Тобаго, Ямайка.

Дээр дурдсан 76 улсын жагсаалтад манай улсыг багтаасан байх бөгөөд Монгол Улсын Үндэсний аюулгүй байдлын үзэл баримтлал (2010) болон

[9] U.S. International Strategy for Cyberspace. 2011.05. p.25

https://www.whitehouse.gov/sites/default/files/rss viewer/intemational strategy for cyberspace.pdf

[10] Derek S. Reveron. “An Introduction to National Security and Cyberspace”, pp. 3-20. Cyberspace and National Security: threats, opportunities, and power in a virtual world / Derek S. Reveron, editor. Georgetown University. Washington DC. 2012. p.3

[11] Cyber Security Strategy Documents. NATO Cooperative Cyber Defence Centre of Excellence. 2016.04

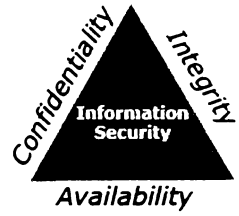
https://ccdcoe.org/cvber-securitv-strategy-documents.html

Мэдээллийн аюулгүй байдлыг хангах үндэсний хөтөлбөр (2010)-г оруулсан байгаа нь НАТО-гийн Кибер довтолгооноос хамгаалах хамтын ажиллагааны төв (CCDCOE)-өөс бэлтгэсэн улс орнуудын кибер аюулгүй байдлын бодлого, эрх зүйн баримт бичгийн жагсаалт үнэхээр шинэлэг бөгөөд бүрэн болохыг харуулж байна.

Улс орнуудын кибер аюулгүй байдлын бодлого, эрх зүйн баримт бичгийг үнэлж цэгнэхэд, “CIA” гурвалжингийн зарчмыг баримтлах шаардлагатай болохыг мэдээллийн аюулгүй байдлын судлаачид тэмдэглэсэн байдаг[12].

Энэ нь мэдээллийн нууцлал *(confidentiality),* бүрэн бүтэн байдал *(integrity),* хүртээмжтэй байдал *(availability)* харилцан тэнцвэртэй, гурвалжингийн тал мэт байх тухай үзэл санаа юм[13].

Хүснэгт 1. Кибер аюулгүй байдлыг хангах зарчим

Бүрэн бүтэн байдал	Мэдээлэл, мэдээллийн орчин, түүний дэд бүтцэд хууль бусаар нөлөөлөх, өөрчлөх оролдлогоос хамгаалж чадсанаар мэдээллийн бүрэн бүтэн байдал хангагдана.	
Нууцлал	Мэдээлэл, түүний бүрдэл хэсэгт хууль бусаар хандах, халдах, задруулахаас хамгаалснаар нууцлал хангагдана.	
Хүртээмж-тэй байдал	Хуулиар хориглоогүй мэдээллийг чөлөөтэй хайх, олж авах, үүсгэх, дамжуулах, түгээх эрх, эрх чөлөөг хангах, мэдээллийн дэд бүтэц, түүний бүрдэл хэсэг, үйлчилгээнд чөлөөтэй хандах боломж бүрдүүлснээр мэдээллийн хүртээмжтэй байдал хангагдана.	

[12] Anthony Henderson. The CIA Triad: Confidentiality, Integrity, Availability. Panmore Institute. 2015.07
http://panmore.com/the-cia-triad-confidentiality-integrity-availability

[13] Энэ талаар Монгол Улсын Үндэсний аюулгүй байддын үзэл баримтлалын 3.6.2, 3.6.3, 3.6.4-д заасан. Монгол Улсын Их Хурлын 2010 оны 48 дугаар тогтоолын хавсралт Монгол Улсын үндэсний аюулгүй байдлын үзэл баримтлал. http://legalinfo.mn/annex/details/3350?lawid=6163

Хоёр. Монгол Улс, ОХУ, БНХАУ-ын цахим орчинд үндэсний аюулгүй байдлыг хангах бодлого, зохицуулалт

Энэ хэсэгт Монгол Улс болон хөрш хоёр орон болох ОХУ, БНХАУ-ын цахим орчинд үндэсний аюулгүй байдлыг хангахтай холбогдсон бодлого, эрх зүйн зохицуулалтаас тэдгээрийн онцлогийг тодорхойлох юм.

Монгол Улсын бодлого, эрх зүйн зохицуулалт

Монгол Улсын хувьд, кибер аюулгүй байдлыг хангах бодлогын үндсэн баримт бичиг нь, 2010 онд шинэчилж боловсруулсан, “Монгол Улсын Үндэсний аюулгүй байдлын үзэл баримтлал” юм[14].

Монгол Улс даяар дагаж мөрдөх цахим засаг, мэдээллийн аюулгүй байдлын нэгдсэн бодлогыг “Үндэсний аюулгүй байдлын үзэл баримтлал”-д тусгасан. Монгол Улсын Их Хурлын 2010 оны 48 дугаар тогтоолын хавсралт "Монгол Улсын Үндэсний аюулгүй байдлын үзэл баримтлал”-д /3.6/ ‘Мэдээллийн салбарт үндэсний ашиг сонирхлыг хамгаалах, төр, иргэн, хувийн хэвшлийн мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдлыг баталгаажуулах нь мэдээллийн аюулгүй байдлыг хангах үндэс мөн” гэж заасан.

Энэ тухай 1994 оны “Монгол Улсын Үндэсний аюулгүй байдлын үзэл баримтлал”-ын[15] 7 дугаар зүйлд тусгагдсан боловч өнөөгийнх шиг мэдээллийн дайны төвшинд асуудал дэгдээгүй байсан. Тиймээс мэдээлэл өөрөө үндэсний аюулгүй байдалд шууд нөлөөлөх үйлчлэл нь бага байсан юм. Дээрээс нь Монгол Улсад мэдээллийн хандлага, түрэмгийлэл ноцтой болчихоод байхад энэ талын ямар ч бичиг баримт байгаагүй учраас, ийм байдлаар мэдээллийн аюулгүй байдлын гол асуудлыг Үндэсний аюулгүй байдлын үзэл баримтлалд тодруулан тусгасан байна[16].

Үүнээс гадна манай Засгийн газрын 2010 оны 141 дүгээр тогтоолын 1 дүгээр хавсралтаар “Мэдээллийн аюулгүй байдлыг хангах үндэсний хөтөлбөр”, 2 дугаар хавсралтаар тус хөтөлбөрийг хэрэгжүүлэх арга хэмжээний төлөвлөгөөг тус тус батласан[17]. Энэ хөтөлбөрийг 2010-2015 онд хэрэгжүүлэхээр төлөвлөсөн бөгөөд 2016 оноос эхлэн кибер аюулгүй байдлыг

[14] National Security Concept of Mongolia. 2010. http://www.nsc.gov.mil/sites/default/files/images/National%20Securitv%20Concept%20of%20Mongolia% 20EN.pdf

[15] Улсын Их Хурлын 1994 оны 6 дугаар сарын 30-ны өдрийн 56 дугаар тогтоолын 1 дүгээр хавсралт. Энэ хавсралтыг 2010 оны 7 дугаар сарын 15-ны өдрийн 48 дугаар тогтоолоор хүчингүй болсонд тооцсон.

[16] Монгол Улсын Ерөнхийлөгчийн Үндэсний аюулгүй байдлын бодлогын зөвлөх М.Батчимэг: Засаглалын маргаанд үндэсний аюулгүй байдлын үзэл баримтлал цэг тавьлаа. 2010.10.21 http://www.president.nui/content/1229

[17] Монгол Улсын Засгийн газрын “Үндэсний хөтөлбөр батлах тухай (мэдээллийн аюулгүй байдал)" 2010 оны 141 дүгээр тогтоол. http://legalinfo.mn/law/details/4716

хангахтай холбоотой, Үндэсний аюулгүй байдлын үзэл баримтлалаас өөр бие даасан бодлогын баримт бичиг үгүй байгаа юм.

Кибер аюулгүй байдлыг хангах нь нэг удаагийн шинжтэй үйлдэл биш бөгөөд кибер халдлага улам бүр бэлтгэгдсэн, хохирол ихтэй болж байгаа тул улс орнууд кибер аюулгүй байдлыг хангах ажиллагааг цаг ямагт, тасралтгүй, идэвхитэй өрнүүлэх хэрэгтэй болдог, гэж судлаачид тэмдэглэсэн байдаг[18].

Гэхдээ, Монгол Улсын ерөнхийлөгчөөс, 2016.02.05-ны өдөр Улсын Их Хуралд "Мэдээллийн аюулгүй байдлын тухай" болон холбогдох бусад хуулийн төслийг өргөн мэдүүлсэн бөгөөд түүнийг Улсын Их Хурлын Аюулгүй байдал, гадаад бодлогын байнгын хороо 2016.04.05-ны өдрийн хуралдаанаар авч хэлэлцээд Улсын Их Хурлын чуулганы нэгдсэн хуралдаанд оруулж хэлэлцүүлэх нь зүйтэй, гэсэн санал гаргасан[19]. Энэхүү хуулийн төсөл нь мэдээллийн аюулгүй байдлыг хангах тогтолцоо, мэдээллийн аюулгүй байдлыг хангах ажиллагааны эрх зүйн үндсийг тодорхойлж, тэдгээртэй холбогдох бусад харилцааг зохицуулах зорилго тавьсан байна. Энэ нь уг хуулийн төсөл батлагдаж хууль болсноор Монгол Улс кибер аюулгүй байдлаа хангахад, дотооддоо дагаж мөрдөх хэм хэмжээтэй болохыг харуулж байна.

ОХУ-ын бодлого, эрх зүйн зохицуулалт

ОХУ-ын хувьд дараах баримт бичигт кибер аюулгүй байдлыг хангах бодлогыг тодорхойлжээ. Үүнд:

- ОХУ-ын Үндэсний аюулгүй байдлын стратеги (2015)[20];
- ОХУ-ын Цэргийн номлол (2014)[21];
- ОХУ-ын Гадаад бодлогын үзэл баримтлал (2013)[22];
- Үндэсний аюулгүй байдлын стратеги 2009-2020 он (2008)[23];
- ОХУ-ын Үндэсний аюулгүй байдлын үзэл баримтлал (2000)[24];

[18] IT Expert underlines the need for firm cyber security measures and public awareness. The UB Post.
2016.03.14 http://ubpost.mongolnews.mn/?p= 18801

[19] Мэдээллийн аюулгүй байдлын тухай хуулийн төсөл. Монгол Улсын Их Хурлын цахим хуудас. 2016.04.05.http://www.parliament.inn/laws/projects/814

[20] Стратегия национальной безопасности Российской Федерации /Утверждена Указом Президента
Российской Федерации от 31 декабря 2015 г. №683
http://static.kremlin.ru/media/events/files/ru/18iXkR8XLAtxeilX7JK3XXy6Y0AsHD5v.pdf

[21] Военная доктрина Российской Федерации /Утверждаю Президент Российской Федерации В.Путин/ http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf

[22] Концепция внешней политики Российской Федерации /Утверждена Президентом Российской Федерации В.В.Путиным 12 февраля 2013 г./
http://archive.mid.rU//brp4.nsf/0/6D84DDEDEDBF7DA644257B 160051BF7F

[23] National Security Strategy of the Russian Federation to 2020 /Approved by Decree of the President
Of the Russian Federation 12 May 2009 No. 537/ http://rustrans.wikidot.com/russia-s-national-security-strategy- to-2020 Стратегия национальной безопасности Российской Федерации до 2020 года

- ОХУ-ын Мэдээллийн аюулгүй байдлын номлол (2016)[24][25] ;

- Олон улсын мэдээллийн аюулгүй байдлын салбар дахь ОХУ-ын төрийн бодлогын үндсэн зарчмууд (2013)[26];

- Мэдээллийн орчин дахь ОХУ-ын зэвсэгт хүчний үйл ажиллагааны баримтлал (2011)[27];

- ОХУ-ын кибер аюулгүй байдлын стратегийн үзэл баримтлалын төсөл (2014.01)[28].

Эндээс харахад, ОХУ-ын хувьд 2000 оноос эхлэж цахим орчинд үндэсний аюулгүй байдлаа хангахтай холбоотой тусгайлсан бодлого баримтлаж ирсэн байх бөгөөд түүнийг цаг үеийн нөхцөлд тааруулж тусгайлан тодруулах зорилгоор ОХУ-ын кибер аюулгүй байдлын стратегийн үзэл баримтлалтай болохын тулд 2014 оноос төлөвлөж, холбогдох төслийг боловсруулжээ. Тус үзэл баримтлалын төсөлд зааснаар дараах үйл ажиллагааг нэн тэргүүнд хэрэгжүүлэх нь зүйтэй гэж үзсэн байдаг. Үүнд,

1) кибер халдлагын эсрэг үндэсний хамгаалалтын тогтолцоог хөгжүүлэх, кибер аюулыг сэрэмжлүүлэх аюулгүй байдлын хувийн тогтолцоог бүрдүүлж, боловсронгуй болгох;

2) онц чухал дэд бүтцийн найдвартай байдлыг хангах техник, тоног төхөөрөмжийг нэмэгдүүлэх шаардлагатай арга хэмжээ авч, тухай бүр боловсронгуй болгох;

3) цахим орчинд олон нийтийн аюулгүй байдлыг хангахад чиглэсэн мэдээллийн нөөц бүрдүүлэх;

4) кибер аюулгүй байдлын салбарт төр, хувийн хэвшил, иргэний нийгмийн түншлэлийг бэхжүүлэх;

5) цахим орчинд аюулгүй байдлын зөв хэвшлийг таниулах, иргэдэд цахим орчны боловсрол олгох ажиллагааг идэвхижүүлэх;

[24] National Security Concept of the Russian Federation /Approved by Presidential Decree No. 24 of 10 January 2000 /http://archive.mid.ru//bdomp/nsosndoc.nsf71e5f0de28fe77fdcc32575d900298676/36aba64ac09f737fc32575d9002bbf31!openDocument

[25] Doctrine of Information Security of the Russian Federation /Approved by Decree of the President of the Russian Federation No. 646 of December 5, 2016/ http://www.mid.ru/en/foreign policv/official documents/-/asset publisher/CptICkB6BZ29/content/id/2563163

[26] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (Утверждены Президентом Российской Федерации В.Путиным 24 июля 2013 г., № Пр-1753) http://www.scrf.gov.rU/documents/6/l 14.html

[27] Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (Unofficial translation by NATO CCDCOE) https://ccdcoe.org/strategies/Russian Federation unofficial translation.pdf

[28] Концепция Стратегии Кибербезопасности Российской Федерации (Проект). http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

6) олон улсын түвшинд кибер аюулгүй байдлыг бэхжүүлэх арга зам, хөгжлийн төлөө гэрээ, хэлэлцээр байгуулах олон улсын хамтын ажиллагааг бэхжүүлэх[29].

БНХАУ-ын бодлого, эрх зүйн зохицуулалт

НАТО-гийн Кибер довтолгооноос хамгаалах хамтын ажиллагааны төв (CCBCOE)-ийн судалгаагаар БНХАУ-ын хувьд дараах баримт бичигт кибер аюулгүй байдлыг хангах бодлого, эрх зүйн зохицуулалтыг тусгасан, гэжээ. Үүнд,

Үндэсний аюулгүй байдлын стратегийн чиглэл (2015);

Үндэсний цэргийн стратеги (2014)[30];

Хятадын төрийн мэдлийн "Синхуа" агентлагийн мэдээлснээр, БНХАУ-ын Үндэсний аюулгүй байдлын стратегийн чиглэлийг, Хятадын коммунист намын Төв хорооны Улс төрийн товчооны 2015.01.23-ны өдрийн хурлаар БНХАУ-ын Ардын их хурлын Байнгын хороо, Төрийн зөвлөл, БНХАУ-ын Ардын улс төрийн зөвлөлдөх бага хурал, Ардын Дээд прокурорын газраар хэлэлцүүлж батласан байна[31]. Харин Синхуа агентлагийн хувьд Хятадын уламжлалт бус аюулгүй байдлын сорилт буюу Хятадын засгийн газрын хувьд онцгой анхаарах болсон кибер халдлага, терроризм зэрэг шинэ аюул заналын талаар ямар нэг байдлаар тоймлоогүй байна. Кибер аюулгүй байдлыг хэрхэн хангах, эс хангах асуудал тус стратегийн чиглэлийн үндсэн хэсэг болсон эсэх нь олон нийтэд ил болоогүй байгаа юм[32].

БНХАУ-ын Батлан хамгаалах яамнаас, БНХАУ-ын Үндэсний цэргийн стратегийг олон нийтэд 2015.05.26-ны өдөр танилцуулсан. Тус стратеги нь оршлоос гадна үндсэн зургаан хэсэгтэй[33]. Үүнд,

1. Үндэсний аюулгүй байдлын нөхцөл байдал;
2. Хятадын Зэвсэгт хүчний эрхэм зорилго, стратегийн зорилт;
3. Батлан хамгаалах үйл ажиллагааны стратегийн чиглэл;
4. Хятадын Зэвсэгт хүчнийг бэхжүүлж, хөгжүүлэх нь;

[29] VI. Приоритеты Стратегии в обеспечении кибербезопасности. Концепция Стратегии Кибербезопасности Российской Федерации (Проект). http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

[30] Document: China's Military Strategy. USNI News. May 26, 2015. https://news.usni.org/2015/05/26/document-chinas-military-strategy

[31] 中央政治局审议通过 "国家安全战略纲要". 2015年01月23日18:05 新华社 http://news.sina.com.cn/c/2015-01-23/180531437149.shtml

[32] China's National Security Strategy - The Politburo, headed by Xi Jinping, emphasized the severity of threats facing China's national security By Shannon Tiezzi. January 24, 2015 http://thediplomat.com/2015/01/chinas-national-security-strategy/

[33] Full text: China's Military Strategy (Xinhua). BEIJING - The Information Office of the State Council on Tuesday published a white paper on China's military strategy. 2015.05.26 http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm

5. Цэргийн тэмцэлд бэлтгэх нь;
6. Цэргийн болон аюулгүй байдлын хамтын ажиллагаа.

БНХАУ-ын Үндэсний цэргийн стратегийн 1 дүгээр хэсэгт, кибер аюулгүй байдлыг хангах нөхцөл шаардлагын талаар тодорхойлсон нь онцлог болжээ.

Энд ‘Гадаад болон цахим орчин нь стратегийн өрсөлдөөний хувьд бүх талын хооронд эрх мэдэл олж авах шинэ өндөрлөг болж байна. Мөн дайны хэлбэр нь мэдээлэлжсэн сөргөлдөөн уруу илүү хурдтай хувьсан өөрчлөгдөх болов[34] [35]. Дэлхийн томоохон хүчнүүд үндэсний аюулгүй байдлын стратеги, батлан хамгаалах бодлогоо тодруулж, цэргийн болон хүчний бүтцийн өөрчлөлтийг идэвхижүүлж байна. Дээр дурдсан цэргийн технологи, дайны хэлбэрийн хувьсан буй өөрчлөлт нь зөвхөн олон улсын улс төр, цэргийн байдалд нөлөөлөхгүй бөгөөд Хятадын цэргийн аюулгүй байдалд шинэ, хүнд сорилт болж байна'' гэжээ.

Мөн стратегийн 4 дэх хэсэгт, цахим орчинд үндэсний аюулгүй байдлыг хангах нөхцөл, шаардлагыг авч үзсэн байна. Энд дурдсанаар, “цахим орчин нь эдийн засаг, нийгмийн хөгжлийн шинэ багана төдийгүй үндэсний аюулгүй байдлын шинэ орчин болсон. Цахим орчин дахь өрсөлдөөний, олон улсын стратеги нь улам харгис болж, нэлээд хэдэн улс кибер цэргийн хүчийг хөгжүүлэх болов. Хятад улс “хакерын халдлагын” гол хохирогчдын нэг байх болсон бөгөөд Хятад улсын кибер дэд бүтцийн аюулгүй байдалд ноцтой аюул тулгарсан. Цахим орчин нь цэргийн аюулгүй байдалд илүү жинтэй тусах болсон тул Хятад улс дараах үйл ажиллагааг идэвхийлэн явуулна. Үүнд,

1) кибер хүчний хөгжлийг хурдасгах,
2) цахим орчны нөхцөл байдлын тухай ойлголтыг нэмэгдүүлэх,
3) кибер довтолгооноос хамгаалах чадавхийг сайжруулах,
4) олон улсын кибер аюулгүй байдлыг хангах хамтын ажиллагаанд оролцох,
5) цахим орчин дахь улс орны хичээл зүтгэлд дэмжлэг үзүүлэх,
6) түүнчлэн томоохон кибер хямралыг зогсоох,
7) үндэсний сүлжээг бэхжүүлж, мэдээллийн аюулгүй байдлыг хангах
8) үндэсний аюулгүй байдал, нийгмийн тогтвортой байдлыг хангах .

Гурав. Кибер аюулгүй байдлыг хангах асуудлаарх Монгол Улс, ОХУ, БНХАУ-ын өнөөгийн байдал, чиг хандлага

[34] Кибер дайн, тулаан буюу Cyber war/ Cyber Warfare гэх ойлголтыг энд авч үзсэн бололтой. Л.Г.

[35] IV. Building and Development of China's Armed Forces. Full text: China's Military Strategy (Xinhua). 2015.05.26 http://www.chinadailv.com.cn/china/2015-05/26/content 20820628 4.htm

ОХУ-ын хувьд бодлого, эрх зүйн зохицуулалт төдийгүй цахим орчин дахь өөрийн үйл ажиллагааны хувьд, цахим эринд бодитоор эргэлт буцалтгүй хөл тавьсан, гэж судлаачид тэмдэглэсэн байдаг. Мөн, ОХУ-ын үндэсний аюулгүй байдал нь мэдээллийн аюулгүй байдлыг хангах, технологийн хөгжлийг хурдасгахаас ихээхэн хамааралтай болсон байна[36]. ОХУ-ын цахим орчин дахь идэвхитэй ажиллагаа нь нэн түрүүнд кибер халдлага, кибер хүчний үйлдлээр илрэх болсон, гэж үзэх нь бий[37].

БНХАУ-ын хувьд интернетийн хувьсгал нь, Хятадын эрх мэдэл, хүч чадлын хурдацтай өсөлтийг тэтгэж, геополитик, эдийн засаг болон цэргийн хүчний төв болох аргаар дэлхийн томоохон "кибер хүч" болоход эргэлзэх зүйлгүй болов. Хятадын хувьд мэдээллийн технологийн салбараа дэлхийн хэмжээнд хүчтэй өрсөлдөхүйц болгож хөгжүүлэх замаар, АНУ болон барууны голлох орнуудаас хамаарал багатай байх, дэлхийн интернетийн засаглалд илүү нөлөөтэй болохыг зорьж байгаа нь нууц биш болов[38].

Монгол Улсын хувьд сүүлийн 5 жилд кибер аюулгүй байдлыг хангах буюу цахим орчин дахь хүний эрх, эрх чөлөөг хамгаалах арга зам, туршлагын талаар дотооддоо төдийгүй олон улсын төвшид хэлэлцэх, мэдээлэл солилцох үйл ажиллагаа эрчимжиж байна.

Цахим засгийн үзүүлэлтээр, Монгол Улс, олон улсын төвшинд тогтмол өсч байгаа хэдий боловч үүнийг цахим орчин дахь хүний эрх, эрх чөлөөний бодит баталгаа, гэж үзэхэд зарим бэрхшээлтэй байгаа[39].

Ийм онцлог бүхий гурван улс буюу Монгол Улс, түүний хөрш хоёр орны хувьд, кзарим талаар төвөгтэй байж болзошгүй. Гэхдээ энэ гурван улсын хувьд, кибер аюулгүй байдлын төвшинг үнэлснээр, түүнд нийцсэн, харилцан уялдаатай, тэнцвэртэй харилцаа тогтоож болох юм.

Хүснэгт 2. Монгол Улсын, хөрш хоёр орны болон бусад зарим улсын кибер аюулгүй байдлын төвшин - 2010

Улсын нэр	Үзүүлэлт	Нийт оноо

[36] Nikolas K. Gvosdev. "The Bear goes Digital: Russia and Its Cyber Capabilities", pp. 173-190. Cyberspace and National Security: threats, opportunities, and power in a virtual world / Derek S. Reveron, editor. Georgetown University Press. Washington DC. 2012. p.175, 177

[37] Brandon Valeriano, Ryan Maness. "Persistent Enemies and Cyberwar: Rivalry Relations in an Age of Information Warfare", pp. 139-158. Cyberspace and National Security: threats, opportunities, and power in a virtual world / Derek S. Reveron, editor. Georgetown University Press. Washington DC. 2012. p.148

[38] Nigel Inkster. China in Cyberspace, pp. 191-206. Cyberspace and National Security: threats, opportunities, and power in a virtual world / Derek S. Reveron, editor. Georgetown University Press. Washington DC. 2012. p.2O3

Л.Галбаатар. Монгол Улсын цахим орчны эрх зүйн зохицуулалтын өнөөгийн байдал, чиг хандлага. 2015.04.20 https://lawschool.academia.edu/Galbaatar/ICT-Law https://www.academia.edu/12012730/Mongolian LawRegulationandEnforcementin DigitalEnvironment

	кибер зөрчил	кибер хамаарал	кибер хамгаалалт	
БНХАУ	5	4	6	15
ОХУ	7	5	4	16
АНУ	9	2	4	15
Иран	4	5	3	12
Израйл	8	3	4	15
БНАСАУ	2	9	7	18

2 дугаар хүснэгтэд харуулсан үзүүлэлт, оноог 2010 онд Richard A.Clarke, Robert K.Knake нар "Кибер дайн: Үндэсний аюулгүй байдалд тулгарч буй дараагийн аюул, заналхийлэл ба түүний эсрэг юу хийх вэ?" номондоо танилцуулсан байдаг. Энд “кибер зөрчил”, “кибер хамаарал”, "кибер хамгаалалт" гэсэн 3 үзүүлэлт тус бүрийг 10 оноогоор үнэлж, тухайн улс орон компьютерийн технологиос хамаарал багатай байх тутам “кибер хамаарал" гэсэн үзүүлэлтээр их оноо авах, цахим орчны технологиос илүү хамааралтай улсын хувьд кибер аюулгүй байдал нь илүү эмзэг, эрсдэлтэй байхаар тооцжээ.

Харин “кибер зөрчил” ба “кибер хамгаалалт” гэсэн үзүүлэлтийн хувьд "сайн хамгаалалт гэдэг нь сайн довтолгоо” гэх харьцуулалтанд дүйцэхүйц байдлаар тооцсон байна. Эндээс харахад, манай хөрш хоёр орны хувьд дээр дурдсан гурван үзүүлэлт харьцангуй ойролцоо оноо авсан байх бөгөөд нийлбэр онооны хувьд бараг ижил байна[40].

АНУ-ын, гурван ерөнхийлөгчийн сонгуульт хугацаанд, тэдний ажлын албанд үндэсний аюулгүй байдлыг хангах чиглэлээр ажилласан байдаг судлаач Richard A.Clarkeгийн зүгээс Монгол Улсын кибер аюулгүй байдлын төвшинд ямар оноо өгөхийг бид мэдэх боломжгүй боловч, тэрээр бичсэн номондоо “кибер аюулгүй байдлын хувьд голлох улс орны байдлыг үнэлсэн” гэж тэмдэглэсэн байгааг анхаарч үзвээс Монгол Улсын кибер аюулгүй байдлын төвшин нь хөрш хоёр оронтой ойролцоо байна, гэж тооцох боломжгүйг харуулж байна.

Энэ нь Монгол Улсын зүгээс кибер аюулгүй байдлаа хангах арга хэмжээнд холбогдуулж ОХУ, БНХАУ-тай “кибер зөрчил”, "кибер хамаарал”, “кибер хамгаалалтын” хүрээнд хамтын ажиллагааг хөгжүүлэх, хоёр

[40] Richard A.Clarke, Robert Knake. Cyber War: The Next Threat to National Security and What to Do about It. HarperCollins Publishers. 2010. p.148, Тус номын танилцуулга, шүүмжийг эндээс унших боломжтой:

Georgetown Security Studies Review. Vol. 1 Issue 1. 2013.12.10. “Richard A.Clarke and Robert K K.nake’s “Cyber War: The Next Threat to National Security and What to Do About It” (Harper Collins, 2010) By David Vanca. http://georgetownsecuritvstudiesreview.org/2013/12/10/richard-a-clarke-and-robert-k-knakes-cyber-war-the-next-threat-to-national-securitv-and-what-to-do-about-it-harper-collins-2010/

хөрштэйгээ харилцан ижил тэгш ажиллах нь зүйтэй юм, гэж ойлгогдож байна.

Үүнээс гадна Олон улсын цахилгаан холбооны байгууллагаас "Дэлхий нийтийн кибер аюулгүй байдлын индекс”-ийг санаачлан боловсруулсан байдаг.[41] Энэ индекс нь тухайн улсын кибер аюулгүй байдлын хөгжлийн түвшинг эрх зүйн арга хэмжээ; техникийн арга хэмжээ; байгууллагын бүтэц; чадавхи бэхжүүлэх; олон улсын хамтын ажиллагаа гэсэн таван хүрээнд тодорхойлдог. Тус индексийн 2014 оны үзүүлэлтээр Монгол Улс 0.412 гэсэн оноотойгоор зургаан улсын хамт 16-д эрэмбэлэгдсэн бол ОХУ 0.50 оноотойгоор 12-д, БНХАУ 0.441 гэсэн оноотойгоор 14-д тус тус эрэмбэлэгдсэн байна.[42] Энэ нь Монгол Улс кибер аюулгүй байдлыг хангах, хөгжүүлэх чиглэлийг тодорхойлсон ач холбогдолтой үзүүлэлт байж болохоор байна.

Харин, манай хөрш хоёр орон, Монголтой кибер аюулгүй байдлын асуудлаар харилцах, энэ харилцааг өргөжүүлэх асуудал нь, манай улсын гуравдагч хөрш болох Япон, АНУ-тай тогтоосон харилцааг сулруулж болзошгүй гэж зарим шинжээч үзсэн байдаг[43]. Мөн Монгол Улс хөрш хоёр орныхоо аль нэгэнтэй нь л илүү ойртох аваас Монголын хувьд аюултай байж болзошгүй гэжээ[44]. Монгол Улсын хувьд хөрш хоёр орныхоо харилцаанд тэнцвэрээ байнга хадгалж, гуравдагч хөрш болох Япон, Өмнөд Солонгос, Канад, АНУ зэрэг улсаас тусламж авах бодлогоо цаашид баримтлах хандлагатай байгаа. Энэ нь өөр нэг улсыг хөрш хоёр орноосоо илүүд үзнэ, гэсэн санаа биш, гэж ойлгогдохоор байна[45].

Нөгөө талаар хүний оршихуйд заналхийлж буй уламжлалт бус аюул занал буюу үндэстэн дамнасан гэмт хэрэг *(кибер гэмт хэрэг)* нь Азийн улс

Global Cybersecurity Index http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Global Cybersecurity Index DM365 Signed.pdf; http://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI.pdf

[42] Global 2014 results http://www.itu.int/en/ITU-D/Cybersecuritv/Documents/GCI Global 2014 results.pdf

[43] Borujigin-Fusure. Хятад Орос, Монгол Улстай харилцаагаа бэхжүүлж байна. 2015.01.14. (Япон хэлнээс товчлон орчуулж бэлтгэсэн Геополитикийн судалгааны хүрээлэнгийн гишүүн судлаач Л.Цагаансанаа). Геополитикийн судалгааны хүрээлэн, 'Геополитик судлал”, №2, 2015 он. Улаанбаатар. 2015. 19 дэх тал.

[44] Gabriel Dominguez. Орос, Хятадтай харилцах Монгол Улсын тэнцвэрт бодлого. 2014.10.05. Геополитикийн судалгааны хүрээлэн, “Геополитик судлал”, №2, 2015 он. Улаанбаатар. 2015.
15-16 дахь тал.

[45] Д.Мягмар. Гурван талт уулзалт болон гурван улсын харилцааны өнөөгийн байдал, ирээдүйн хандлага.
2014.10.31. Геополитикийн судалгааны хүрээлэн, ‘Геополитик судлал”, №1, 2015 он. Улаанбаатар. 11 дэх тал

орнуудын аюулгүй байдалд шинэ сорилт болж байна[46]. Иймд Монгол Улс, хөрш хоёр оронтойгоо кибер аюулгүй байдлыг хангах асуудлаар харилцах, хамтран ажиллахын өмнө Азийн бусад улсын кибер аюулгүй байдлыг хангах асуудлаар хоёр талт харилцаанаас туршлага судлах нь зүйтэй санагдана. Өнөөдрийн байдлаар Ази тивд дараах улс орнууд кибер аюулгүй байдлыг хангах хоёр болон гурван талт харилцааг бусад улс оронтой хөгжүүлсээр байна.

3 дугаар хүснэгтэд үзүүлснийг харахад, Азийн улс орнуудын кибер аюулгүй байдлыг хангах хоёр болон гурван талт харилцааны гол тоглогчид нь АНУ, Япон, БНСУ, ОХУ, БНХАУ, Австрали, Эстон байх бөгөөд 2009 оноос эхлэн улс орнууд кибер аюулгүй байдлаа хангах чиглэлээр хамтран ажиллах, харилцан үүрэг хүлээх болсон байна.

Кибер аюулгүй байдлын асуудал дээр АНУ ба Японы эвслийн талаар бичсэн бүтээлдээ улс төр-цэргийн нэрт судлаач, доктор James Andrew Lewis кибер аюулгүй байдлыг хангахад улс орнуудын хоёр талт харилцаанд дараах гол гурван чиглэлээр онцгой анхаарах хэрэгтэй, гэж тэмдэглэсэн байдаг[47]. Үүнд,

1) Цэргийн хамтын ажиллагааг өргөжүүлэх;

2) Онцгой ач холбогдолтой дэд бүтцийг хамгаалахад үндэсний хэмжээнд төдийгүй нөгөө талтайгаа хамтарч илүү хүчин чармайлт гаргах;

3) Кибер аюулгүй байдлын хангахад, хүний нөөц ихтэй болох.

Хүснэгт 3. Азийн улс орнуудын, кибер аюулгүй байдлаа хангах хоёр болон гурван талт харилцааны байдал

Талууд	Зарласан огноо	Эхлэл	Зорилго, чиглэл
АНУ ОХУ	2013.6.17	2013	Мэдээлэл, харилцаа холбооны салбарт хамтран ажиллах асуудлаар хэлэлцээ хийх төрийн төвшний уулзалт[48]
БНХАУ БНСУ	2014.10.21[49] 2О15.1О.13[50]	2014	БНХАУ, БНСУ, Япон улсууд кибер аюулгүй байдлын зөвлөлдөх механизм бий болгох, кибер

[46] D.Myagmar. New Geopolitical Situation and Defense Policy of Mongolia. 2012. pp. 15-20. The Institute for Geopolitical Studies, “The Mongolian Journal of Geopolitical Studies”, №1, 2015. Ulaanbaatar. 2015. p. 15

[47] James Andrew Lewis. U.S.-Japan Cooperation in Cybersecurity (A Report of the CSIS Strategic Program). November 2015. p. 3 http://csis.org/files/publication/151105 Lewis USJapanCvber Web.pdf

[48] The New Norms: Global Cyber-Security Agreements Face Challenges By Tim Maurer, February 5, 2016 IHS Jane’s Intelligence Review http://camegieendowment.org/2016/02/05/new-norms-global-cvber-securitv-protocols-face-challenges/iv53

[49] China, Japan, ROK hold cyber security meeting in Beijing (Xinhua) 2014.10.22 http://www.chinadailv.com.cn/world/2014-10/22/content 18786642.htm

Япон			гэмт хэрэг, терроризмтой тэмцэхинтернетийн онцгой байдлын үед хариу үзүүлэх асуудлаар хамтран ажиллах[51]
АНУ Япон	2015.4.28[52]	2013[53]	Японы хөрш атлаа кибер халдлагын хамгийн идэвхитэй улс орнууд болох БНХАУ, Хойт Солонгос, ОХУ, Ираны кибер халдлагаас урьдчилан сэргийлэх буюу түүнд хариу үзүүлэх[54]
ОХУ БНХАУ	2015.5.08[55]	2009[56]	Кибер аюулгүй байдлыг хангах, цахим орчинд харилцан үл довтлох[57]
ОХУ	2015.5.08[58]	2009[59]	Кибер аюулгүй байдлыг хангах, цахим орчинд

50 S. Korea, Japan, China to hold cyber policy talks, 2015.10.13 http://english.yonhapnews.co.kr/news/2015/10/13/0200000000AEN20151013004800315 .html?b 1 e 08f30

51 Олон улсын цахилгааны холбооны байгууллага (ITU), Зүүн Өмнөд Азийн улсуудын холбооны бүс нутгийн форум (ASEAN), БРИКС (Бразил, ОХУ, Энэтгэх, БНХАУ, Өмнөд Африкийн 5 улсын бүлэг), Шанхайн Хамтын ажиллагааны байгууллага зэрэг олон улсын байгууллагуудын үйл ажиллагааны хүрээнд кибер аюулгүй байдлын асуудлаар харилцан итгэлцэх зорилготой.

China, Japan, ROK hold cyber security meeting in Beijing (Xinhua) 2014.10.22 http://www.chinadaily.com.cn/world/2014-10/22/content 18786642.htm

China, Japan, South Korea Talk Cyber Issues, By Emilio lasiello, 2015.11.23, DarkMatters-Superior Attack Intelligence. http://darkmatters.norsecorp.com/2015/11/23/cyber-issues-china-japan-south- korea-talk/

52 White House unveils cyber pact with Japan, By Cory Bennett Arpil 28 2015, Th Hill http://thehill.com/policy/cybersecurity/240283-white-house-unveils-unprecedented-cyber-partnership-with-j apan

53 Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group, May 30, 2015 http://www.mod.go.ip/i7press/news/2015/05/30a_1_.pdf Japan and the United States to Deepen Cybersecurity Cooperation: The growing threat of digital attacks moves Washington and Tokyo closer together in trying to secure cyberspace By Franz-Stefan Gady, June 02, 2015 http://thediplomat.com/2015/06/japan-and-the-united-states-to-deepen-cybersecurity-cooperation/

54 James Andrew Lewis. U.S.-Japan Cooperation in Cybersecurity (A Report of the CSIS Strategic Program). November 2015. p. 17 http://csis.0rg/f1les/publicati0n/l 51105_Lewis_USJapanCyber Web.pdf

55 The Next Level for Russia-China Cyberspace Cooperation? By Elaine Korzak, August 20, 2015 http://blogs.cfr.org/cyber/2015/08/20/the-next-level-for-russia-china-cyberspace-cooperation/

56 Шанхайн хамтын ажиллагааны байгууллагын гишүүн орнуудын олон улсын мэдээллийн аюулгүй байдлын салбарт хамтран ажиллах тухай хэлэлцээр - 2009.06.16 (2012.01.05-ны өдөр хүчин төгөлдөр болсон) https://ccdcoe.org/sites/default/files/documents/SCO-09Q616-IISAgreementRussian.pdf

57 Соглашение между Правительством Российской Федерацией и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности, 2 015.04.30 http://govemment.ru/media/files/5AMAccs7mSlXgbfflUa785WwMWcABDJw.pdf

58 The Next Level for Russia-China Cyberspace Cooperation? By Elaine Korzak, August 20, 2015

БНХАУ			харилцан үл довтлох[60]
Австрали БНСУ	2015.9.11[61]	2013[62]	Кибер аюул заналтай холбогдуулж цахим орчин дахь хэм хэмжээний хэлэлцээр, хоёр талт яриа хийх зэргээр цахим орчинд аюулгүй болон нээлттэй байдлыг хангах олон улсын хүчин чармайлтад хувь нэмэр оруулах, цахим орчинд үндэсний аюулгүй байдлыг хангах асуудлаар хамтран ажиллах [63]
АНУ БНХАУ	2015.9.25[64]	2015	Хоёр улсын засгийн газрын аль нь ч тухайн улсын компаниудын хэвийн үйл ажиллагаа, өрсөлдөөнд ач холбогдол бүхий худалдааны болон бизнесийн нууц мэдээлэл зэрэг оюуны өмчийн цахим хулгайг зохион байгуулах буюу мэдсээр байж дэмжихгүй байх;[65] олон улсын хамтын нийгэмлэгийн хүрээнд цахим орчин дахь төрийн үйл ажиллагааны зохистой хэм хэмжээг дэмжих[66];

http://blogs.cfr.org/cvber/2015/08/20/the-next-level-for-russia-china-cyberspace-cooperation/

[59] Шанхайн хамтын ажиллагааны байгууллагын гишүүн орнуудын олон улсын мэдээллийн аюулгүй байдлын салбарт хамтран ажиллах тухай хэлэлцээр - 2009.06.16 (2012.01.05-ны өдөр хүчин төгөлдөр болсон) https://ccdcoe.org/sites/default/files/documents/SCO-09Q616-IISAgreementRussian.pdf

[60] Соглашение между Правительством Российской Федерацией и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности, 2015.04.30 http://govemment.ru/media/files/5AMAccs7mSlXgbfflUa785WwMWcABDJw.pdf

[61] Australia-Republic of Korea Foreign and Defence Ministers 2+2 Meeting, Joint statement. 11 September 2015 http://foreignminister.gov.au/releases/Pages/2015/ib_mr_l_50911_.aspx?w=tb_1_CaGpkPX%2FlS0K%2Bg9ZKEg%_3D%3D

[62] Australia and South Korea to Deepen Defense Ties: The defense and foreign ministers of both countries agreed to a new defense and security cooperation blueprint. By Franz-Stefan Gady. September 17, 2015 http://thediplomat.com/2015/09/australia-and-south-korea-to-deepen-defense-ties/

[63] Энэ хүрээнд кибер халдлыг бүртгэн судлах, хариу үзүүлэх мэргэжлийн багуудын хооронд мэдээлэл солилцох, хамтран ажиллах (KrCERT/CC; CERT Australia), хоёр талын цахим гэмт хэрэгтэй тэмцэх чиглэлийн цагдаагийн албад хооронд хамтын ажиллагааг хөгжүүлэхээр тохиролцсон.

[64] Fact Sheet: President Xi Jinping's State Visit to the United States, September 25, 2015 https://www.whitehouse.gOv/the-press-office/2015/09/25/fact-sheet-president-xi-iinpings-state-visit-united-states

[65] Хоёр тал хор хөнөөл бүхий кибер үйл ажиллагаатай холбоотой тусламж үзүүлэх, мэдээлэл хүсэхэд цаг тухайд нь хариу өгч байх, түүнчлэн холбогдох үндэсний хууль тогтоомж, олон улсын эрх зүйгээр хүлээсэн үүргийн хүрээнд кибер гэмт хэргийг мөрдөн шалгах, цахим нотлох баримт цуглуулах, хоёр талын тухайн нутаг дэвсгэрээс явуулсан хортой кибер үйл ажиллагааг бууруулах асуудалд хамтран ажиллах, кибер гэмт хэргийн мөрдөн шалгалтын явц, үр дүнг нөгөө талд зохих ёсоор мэдээлэхээр тохиролцсон.

[66] АНУ болон БНХАУ нь олон улсын аюулгүй нөхцөл байдал дахь мэдээлэл, харилцаа холбооны салбарын асуудлаарх НҮБ-ын засгийн газрын шинжээчдийн багийн 2015 оны 7

			Кибер гэмт хэрэгтэй тэмцэх болон кибер аюулгүй байдалд холбоотой бусад асуудлаар дээд төвшний яриа, хэлэлцээр хийх механизмыг бий болгох[67]
АНУ БНСУ	2015.10.16 [68]	2013[69]	Хойд Солонгосын кибер халдлагын эсрэг хамтран тэмцэх
Эстони Япон	2016.04.08 [70]	2015	Төр, иргэн, хувийн хэвшлийн өдөр тутмын ажиллагаанд тоон сүлжээг үүсгэж, хэвийн ажиллах нөхцөлийг дэмжих; Токиогийн 2020 оны олимпийн наадмаас өмнө кибер аюулгүй байдлыг бэхжүүлэх.

Монгол Улсын хувьд дээр дурдсан гурван чиглэлээс гадна Шанхайн хамтын ажиллагааны байгууллагын гишүүн орнууд болох ОХУ, БНХАУ, Казахстан, Киргиз, Тажикстан, Узбекистан гэсэн зургаан улс хамтран НҮБ-ын Ерөнхий нарийн бичгийн даргад 2011; 2015 онд өргөн барьсан “Мэдээллийн аюулгүй байдлын асуудлаар баримтлах зан үйлийн олон улсын код”-ыг зайлшгүй харгалзан үзэх нь чухал юм* [67] * [69] [70] [71].

дугаар сарын тайланд тусгасан цахим орчинд олон улсын аюулгүй байдлыг хангахтай холбоотой зан байдлын хэм хэмжээ болон бусад чухал ач холбогдолтой асуудлыг найрсаар хүлээн авах, цаашид тус асуудлаарх яриа, хэлэлцүүлэг хийх зорилгоор ахлах шинжээчдийн баг байгуулахаар хүлээн зөвшөөрсөн.

[67] Ийм яриа, хэлэлцүүлэгт БНХАУ-ын талаас сайд нарын түвшний албан тушаалтнуудыг томилон

оролцуулах бөгөөд Нийтийн аюулгүй байдлын сайд, Төрийн аюулгүй байдлын сайд, Хууль зүйн сайд, Төрийн интернет, мэдээллийн газар хэлэлцүүлгийг даргалан оролцоно. АНУ-ын талаас Дотоод аюулгүй байдлын нарийн бичгийн дарга, Ерөнхий прокурор болон Холбооны мөрдөх товчоо, АНУ-ын тагнуулын байгууллагуудын төлөөлөл хэлэлцүүлгийг хамтран даргалж оролцоно. Энэ яриа, хэлэлцүүлгээр

талуудын зүгээс хортой кибер үйл ажиллагааг бууруулах асуудалд хамтран ажиллах, кибер гэмт хэргийн мөрдөн шалгалтын явц, үр дүнг нөгөө талд зохих ёсоор мэдээлэх үйл ажиллагааны цаг хугацаа, чанарыг хянана. Мөн хоёр тал дурдсан асуудлаар талуудын мэдээлэл солилцох, хамтран ажиллахад зориулсан шууд утас ажиллуулна. Мөн хоёр тал анхны уулзалтыг 2015 оны сүүлээр зохион байгуулах, түүнээс хойш жилд хоёр удаа уулзалт зохион байгуулахаар тохиролцсон.

[68] Remarks by President Obama and President Park of the Republic of Korea in Joint Press Conference. The White House, Oct 16, 2015 https://www.whitehouse.gov/the-press-office/2015/10/16/remarks-president-obama-and-president-park-republic-korea-joint-press

[69] US, South Korea join forces to prevent cyberattacks by North Korea By Jennifer Chang, IDG News Service, Apr 3, 2013 1:25 PM
http://www.pcworld.com/article/2032918/us-south-korea-join-forces-to-prevent-cyberattacks-by-north- korea.html

[70] Japan, Estonia vow to strengthen cybersecurity cooperation. The Japan Times, April 8, 2016
http://www.iapantimes.co.ip/news/2016/04/08/national/politics-diplomacy/japan-estonia-vow-strengthen-cybersecurity-cooperation/#.VwgOIqQrLNN

[71] International code of conduct for information security (Annex to the letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation,

Гэвч. тухайн үед 2011 оны "Мэдээллийн аюулгүй байдлын асуудлаар баримтлах зан үйлийн олон улсын код"-ын төслийг АНУ тэргүүтэй барууны ихэнх орны зүгээс. "...энэхүү баримт бичгийг санаачлагч дөрвөн улс *(БНХАУ, ОХУ. Тажикстпан. Узбекистан)* нийлж, интернетийн засаглалын бүтэц, онлайны контентод төрийн хяналт тавих гэж байна", хэмээн шүүмжилж эсэргүүцсэнээр НҮБ-ын дэмжлэг авч чадаагүй юм[72].

Мөн 2011 оны төслийг шүүмжлэгчид "...олон талт оролцоог үгүйсгэсэн" гэж үзсэн учраас 2015 оны төсөлд "мэдээллийн аюулгүй байдлын олон улсын хэм хэмжээтэй холбоотой олон улсын мэтгэлцээнийг эрчимжүүлж, энэ асуудлаар урьдчилан зөвшилцөхөд туслах" нөхцөлийг хангасан, гэж боловсруулагчид нь тайлбарлажээ[73]. Одоогоор 2015 оны төслийг НҮБ-аас батлаагүй байгаа бөгөөд боловсруулагчид нь төслийн үндсэн санааг дэмжихийг бусад улс орнуудад уриалсан байна[74].

Кибер аюулгүй байдлын асуудал нь зөвхөн Шанхайн хамтын ажиллагааны байгууллагын гипгүүн орнууд боловсруулсан "Мэдээллийн аюулгүй байдлын асуудлаар баримтлах зан үйлийн олон улсын код"-ыг тойрсон хэлэлцүүлгээр хязгаарлагдахгүй, харин ч дэлхийн улс төр, эдийн засаг, мэдээллийн салбарт өдөр ирэх тусам ач холбогдолтой болсоор байна. Тухайлбал, 2016 оны 5 дугаар сард болох Мэдээллийн нийгмийн асуудлаар хийх дэлхийн хэмжээний дээд уулзалт (WSIS)-д оролцогчид, тогтвортой хөгжлийн төлөө кибер аюулгүй байдлын үндэсний стратегийн талаар хэлэлцэх, гэж байна[75]. Мөн Олон улсын цахилгааны холбооны байгууллага

Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General [Original: Chinese and Russian])
https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf
https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/02/PDF/N1501402.pdf?OpenElement
International code of conduct for information security (Annex to the letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General [Original: Chinese, English and Russian])
https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf
http://www.un.org/ga/search/view_doc.asp?symbol=A%2F66%2F359&Submit=Search&Lang=E

[72] Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era? By Alex Grigsby, January 28, 2015 http://blogs.cfr.org/cyber/2015/01/28/will-china-and-russias-updated-code-of-conduct-get- more-traction-in-a-post-snowden-era/

[73] An Analysis of the International Code of Conduct for Information Security. By Sarah McKune September 28, 2015 https://citizenlab.org/2015/09/international-code-of-conduct/

[74] Dmitry Medvedev attends the opening ceremony of the 2nd World Internet Conference. From Dmitry Medvedev's address, 16 Dec 2015, Wuzhen, People's Republic of China http://government.ru/en/news/21075/

[75] WSIS Forum 2016, Draft Agenda (As of 7 April 2016) https://www.itu.int/net4/wsis/forum/2016/Content/documents/agenda/WSISForum_2016_DraftAgenda_ 2016-04-07.pdf

(ITU)-аас "Кибер аюулгүй байдлын үндэсний стратегийн гарын авлага" боловсруулж нийтэд танилцуулсан ажээ[76].

Дүгнэлт

Өнөөдөр цахим орчин нь дэлхийн эдийн засаг, нийгмийн хөгжлийн шинэ тулгуур төдийгүй үндэсний аюулгүй байдлын шинэ орчин болсон учраас ихэнх улс орон, цахим орчин дахь үл ойлголцол, зөрчилдөөнд бэлэн байхыг зорих болов. Энэ нь юуны өмнө цахим орчинд, үндэсний аюулгүй байдлыг хангах бодлогын баримт бичиг боловсруулж батлах, энэ асуудлаар хоёр болон олон талт яриа хэлэлцээ хийх, хамтарсан кибер сургуулилт зохион байгуулах зэргээр илрэх болов.

Үндэсний аюулгүй байдлыг, цахим орчинд хангахтай холбогдуулсан, олон улсын хүчин чармайлтын үр дүнд, улс орнууд кибер аюулгүй байдлаа хангахын тулд мэдээллийн бүрэн бүтэн, нууцлагдсан байдлыг бэхжүүлэх нь зүйтэй, гэдэг дээр санал нэгдэж байгаа хэдий боловч мэдээллийн хүртээмжтэй байдлыг яаж хэрэгжүүлэх талаар санал зөрөлдөж, нээлттэй интернетийг хязгаарлах аливаа санаачлагаас болгоомжилдог байна. Үүний тод жишээ нь, Шанхайн хамтын ажиллагааны байгууллагын гипгүүн орнууд боловсруулсан "Мэдээллийн аюулгүй байдлын асуудлаар баримтлах зан үйлийн олон улсын код"-ыг тойрсон асуудлаар улс орнууд хоёр талт байр суурь баримтлаж байна.

Улс орнуудын кибер аюулгүй байдлыг хангах хоёр болон гурван талт харилцааны гол тоглогчид нь АНУ, Япон, БНСУ, Эстон, Австрали улсаас гадна Монгол Улсын хөрш хоёр орон ОХУ, БНХАУ болжээ.

Ийм харилцаа нь ОХУ ба БНХАУ-ын хувьд, кибер халдлагаас сэргийлэх буюу түүний эсрэг хамтран тэмцэх чиглэлээр хөгжиж байгаа нь ажиглагдаж байна. Энэ нь Монгол Улс кибер аюулгүй байдлыг хангах асуудлаар хөрш хоёр оронтой харилцахдаа тэнцвэрийг хадгалж, цаашид гуравдагч хөрш буюу Япон, Өмнөд Солонгос, АНУ зэрэг улсаас дэмжлэг авах бодлого баримтлах нь зүйтэй гэдгийг харуулж байна.

Энэхүү нарийн төвөгтэй байдал нь, Монгол Улсын хувьд бусад улс орон, олон улсын байгууллагаас боловсруулсан кибер аюулгүй байдлын бодлого, үйл ажиллагааны баримт бичигт уялдуулсан бөгөөд өөрийн орны "Үндэсний аюулгүй байдлын үзэл баримтлал"-д нийцүүлсэн "Кибер аюулгүй байдлын үндэсний стратеги"-ийг гаргаж ирэх хэрэгцээг бий болгож байгааг анхаарч үзэх хэрэгтэй байна.

Цаашид Монгол Улс "Дэлхий нийтийн кибер аюулгүй байдлын индекс" дэх байраа ахиулах, үүний тулд кибер аюулгүй хангах чиглэлээр эрх

[76] The ITU National Cybersecurity Strategy Guide. Dr. Frederick Wamala (Ph.D.), CISSP®. Geneva, 2012
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

зүй. техникийн арга хэмжээ авах, энэ чиглэлийн байгууллагуудын бүтэц, зохион байгуулалтыг сайжруулах төдийгүй олон улсын хамтын ажиллагааг өргөжүүлэх шаардлагатай байна.