КИБЕР ГЭМТ ХЭРЭГТЭЙ ТЭМЦЭХ ОЛОН УЛСЫН ТУРШЛАГА БА ЭРХ ЗҮЙН ОРЧИН

О.Билгүүтэй, Р.Оргилмаа, Б.Батцэцэг

АГУУЛГА

УДИРТГАЛ

Улсын Их Хурлын гишүүний захиалгаар “Кибер гэмт хэрэгтэй тэмцэх олон улсын туршлага ба эрх зүйн орчин” сэдэвт судалгааны ажлыг Парламентын судалгааны хүрээлэнд гүйцэтгэв.

Судалгааны зорилго: Цахим орчинд үйлдэгдэж буй кибер гэмт хэргийн талаарх нийтлэг ойлголт, гэмт хэргийн төрөл, хэлбэр, цахим гэмт хэрэгтэй тэмцэх асуудлаарх олон улсын зөвлөмж, бусад орнуудын туршлага болон эрх зүйн орчныг харьцуулан судлах.

Судалгааны хүрээ: Судалгаанд кибер аюулгүй байдал, цахим гэмт хэргээс урьдчилсан сэргийлэх бодлого, стратеги, эрх зүйн орчин сайтай өндөр хөгжилтэй орнууд болох АНУ, ИБУИНХУ, БНСУ, Малайз, Япон, Герман зэрэг 6 орныг сонгон авч бодлого, эрх зүйн орчны хүрээнд харьцуулан судлав. Эдгээр орнуудын цахим орчин дахь гэмт хэргийн нөхцөл байдал, цахим гэмт хэрэгтэй тэмцэх чиглэлээр баримталж буй бодлого, стратеги төлөвлөгөө болон институциональ тогтолцоо, эрх зүйн орчны асуудлуудыг авч үзсэн.

Түүнчлэн сэдвийн хүрээнд кибер аюулгүй байдлыг хангах, цахим гэмт хэрэгтэй тэмцэх чиглэлээр олон улсын холбогдох байгууллагуудаас гаргасан зөвлөмж, олон улсын гэрээ, конвенцууд болон уг асуудалтай холбоотой олон улсын нэр томьёоны тодорхойлолт, үндсэн ойлголтуудыг авч үзсэн болно.

Судалгааны бүтэц: Судалгааны мэдээллийг дараах 4 бүлэг асуудлын хүрээнд ангилан боловсруулсан:

- Кибер гэмт хэрэг, халдлагын тухай ерөнхий ойлголт
- Кибер аюулгүй байдлын олон улсын зохицуулалт
- Монгол Улс дахь кибер аюулгүй байдал
- Гадаадын зарим орны туршлага

СУДАЛГААНЫ ХУРААНГУЙ

Сүүлийн жилүүдэд цахим орчинд үйлдэгдэж буй гэмт хэргийн нэр төрөл, арга, хэлбэр улам нарийсч, ийм төрлийн гэмт хэргийн гаралт ихсэж байна.

Иймд дэлхийн улс, орнууд кибер гэмт хэрэгтэй тэмцэх үндэсний бодлого стратегиа тодорхойлж, хүний нөөцөө бэлтгэх, хамгаалалтын дэд бүтэц бий болгох, байгууллага бүр дотооддоо бодлогын баримт бичиг, журам заавар батлан мөрдөх, эрсдлийн үнэлгээ хийх, аудит дээр суурилсан хамгаалалтын шийдлүүд гарган хэрэгжүүлэх, цахим гэмт хэрэгтэй тэмцэх үндэсний тогтолцоогоо бий болгох, эрх зүйн орчныг бүрдүүлэхээс гадна бүх нийтийн мэдлэг, ойлголтыг дээшлүүлэх гэх мэт арга хэмжээнүүдийг авах замаар энэ төрлийн гэмт хэрэгтэй тэмцэж байна.

Судалгааны нэгдүгээр бүлэгт, кибер гэмт хэрэг, кибер халдлагын тухай ерөнхий ойлголт, мэдээллийг оруулсан. Системийн сул талыг ашиглан хувь хүн, аж ахуйн нэгж, цаашлаад улсын нууцын зэрэглэлтэй мэдээлэл рүү нэвтэрч халдлага үйлдэх гэмт хэргүүд ихээр гарах болсон. Иймд цахим гэмт хэргийн нэр төрөл, халдлагын хэлбэр, халдлага үйлдэх арга замуудын талаар олон улсын хэмжээний зарим гол ойлголтууд болон нэр томьёоны тодорхойлолтыг энэ бүлэгт авч үзсэн болно.

Хоёрдугаар бүлэгт, олон улсад мөрдөж байгаа кибер аюулгүй байдлыг хангахтай холбоотой дараах стандарт, бодлогын зөвлөмж болон олон улсын гэрээ конвенцуудын талаарх мэдээллийг тусгасан.

- Олон улсад одоогоор кибер аюулгүй байдалтай холбоотой ISO/IEC 27032:2012 болон ISO 27001 стандартуудыг мөрдөж байна.
- Аливаа улс орны цахим халдлагаас өөрийгөө хамгаалах чадамжийг Олон улсын харилцаа холбооны байгууллагаас гаргасан “Кибер аюулгүй байдлын индекс”-ээр тодорхойлдог байна. Уг индексийг (1) эрх зүйн орчин (2) техникийн арга хэмжээ, (3) байгууллагын зохион байгуулалтын арга хэмжээ, (4) чадавх бэхжүүлэх арга хэмжээ, (5) хамтын ажиллагаа гэсэн үндсэн 5 чиглэлээр багцлан тодорхой шалгуур үзүүлэлтүүдээр гаргадаг.
- Олон улсын Програм хангамжийн холбоо (BSA)-ноос гаргасан зөвлөмжид кибер аюулгүй байдалтай холбоотой бодлого боловсруулахад дэлхийн улс орнуудын засгийн газруудаас баримтлах 6 тулгуур зарчмыг тодорхойлсон.
- 2001 онд “Кибер гэмт хэрэгтэй тэмцэх тухай Будапештийн конвенц” батлагдаж 2004 оноос эхлэн хэрэгжиж эхэлсэн бөгөөд энэхүү конвенцын зорилго, ач холбогдол, нэгдэн орсноор бий болох давуу талуудын талаарх мэдээллийг мөн энэ бүлэгт тоймлон оруулсан.

Гуравдугаар бүлэгт, Монгол Улс дахь кибер аюулгүй байдлын эрх зүйн орчин, кибер аюулгүй байдлыг хангахтай холбоотой үндэсний аюулгүй байдлын үзэл баримтлал болон холбогдох хуулийн зохицуулалт, хэрэгжилтийг хариуцаж буй байгууллагуудын талаарх мэдээллийг тоймлон оруулсан.

Дөрөвдүгээр бүлэгт, Кибер аюулгүй байдлын индексээр дэлхийд тэргүүлдэг, цахим гэмт хэрэгтэй тэмцэх хууль, эрх зүйн зохицуулалт сайтай АНУ, ИБУИНХУ, БНСУ, Малайз, Япон, Герман зэрэг орнуудыг сонгон авч кибер гэмт хэрэгтэй тэмцэх чиглэлээр хэрэгжүүлж буй бодлого стратеги болон холбогдох эрх зүйн зохицуулалтыг дэлгэрүүлэн судалсан болно.

Судалгаанд авагдсан орнуудын туршлагыг тоймлон танилцуулбал:

АНУ: Цахим гэмт хэрэгтэй тэмцэх “Үндэсний цахим стратеги”, “Богино хугацааны үндэсний аюулгүй байдлын стратегийн удирдамж”, “Үндэсний цахим аюулгүй байдлыг сайжруулах тухай” Ерөнхийлөгчийн зарлиг зэрэг хэд хэдэн бодлогын баримт бичгүүдийг батлан хэрэгжүүлж байна. Холбооны Засгийн газрын харьяа агентлагууд улс орны эдийн засгийн аюулгүй байдлыг хангах үүднээс томоохон дэд бүтцийн байгууламжууд, үйлдвэр үйлчилгээний газрууд, цаашлаад цахим сүлжээнд холбогдсон улсын болон хувийн байгууллагуудад Үндэсний стандарт технологийн хүрээлэнгээс батлан гаргасан нийтээр дагаж мөрдөх цахим аюулгүй байдлын нэгдсэн стандартыг дагаж мөрдөхийг шаарддаг. Түүнчлэн цахим аюулгүй байдлыг хамгаалах мэдлэг чадвартай хүний нөөцийг бүрдүүлэхэд анхаардаг.

АНУ-д одоогоор цахим орчны аюулгүй байдлын тухай 18 хуулийн төсөл Конгресст өргөн баригдаад байна.[398] Цахим гэмт хэргийн хохирогчдын ихэнх хувийг хүүхэд, өсвөр насныхан

[398] https://www.washingtonpost.com/politics/2021/10/18/cybersecurity-legislation-is-waiting-wings/

эзэлдэг тул хүүхэд, залуусыг цахим гэмт хэргээс урьдчилан сэргийлэх, хамгаалах хууль цөөнгүй байна. Цахим харилцаанд оролцож буй талууд, ялангуяа интернэтээр үйлчилгээ үзүүлэгч байгууллагуудын үүрэг, хариуцлагыг эдгээр хуулиудад тодорхой тусгаж өгчээ.

ЯПОН УЛС: 2021 оны 9 дүгээр сард Кибер аюулгүй байдлын 3 дахь стратеги төлөвлөгөөг нийгэм- эдийн засгийн тогтвортой хөгжлийг хангах, аюулгүй байдал-дижитал нийгмийг ухамсарлах, Япон Улсын үндэсний аюулгүй байдлыг хангах гэсэн 3 чиглэлээр хэрэгжүүлэхээр баталсан байна. Энэхүү төлөвлөгөө болон бусад бодлогын баримт бичгийн хүрээнд Японы Цагдаагийн ерөнхий газар, Кибер гэмт хэрэгтэй тэмцэх төв, Засгийн газрын хэрэг эрхлэх газар, холбогдох яамд болон интернэт орчинд үйл ажиллагаа явуулдаг хувийн хэвшлийн холбоо болох “Өсвөр үеийнхний интернэт ашиглалтыг сайжруулах зөвлөл” гэх мэтийн олон байгууллагууд хамтран ажилладаг.

Япон улсад кибер гэмт хэрэгтэй тэмцэх харилцааг Эрүүгийн хууль, Хүүхдийн биеийг үнэлэх, садар самуунд уруу татсан үйлдэлд хариуцлага ногдуулах болон хүүхэд хамгаалах тухай хууль, Насанд хүрээгүй хүмүүст интернэтийн аюулгүй орчныг бүрдүүлэх тухай хууль, Зөвшөөрөлгүйгээр цахим сүлжээнд нэвтрэхийг хориглох тухай хууль болон Кибер аюулгүй байдлын тухай хуулиар тус тус зохицуулж байна.

ГЕРМАН УЛС: “Кибер аюулгүй байдал-2021” стратеги төлөвлөгөөнд хамтын хариуцлагын хүрээнд цахим аюулгүй байдлыг бүрдүүлэх, төр, бизнес, шинжлэх ухаан, нийгмийн цахим халдашгүй байдлыг бэхжүүлэх, цахим хөгжлийн аюулгүй байдлыг хангах, хэмжигдэхүйц хийгээд ил тод болгох гэсэн 4 чиглэлийн дагуу холбогдох арга хэмжээнүүдийг авч хэрэгжүүлж байна.

Холбооны улсын Хууль зүйн яам, Гэр бүлийн яам, Цагдаагийн байгууллага, Эрүүгийн цагдаагийн газар зэрэг төрийн захиргааны байгууллагууд хамтран цахим гэмт хэргийн талаарх үйл ажиллагааг хянах, мэдээллийг индексжүүлэх, санал гомдол хүлээн авах, шийдвэрлэх, цахим гэмт хэргээс урьдчилан сэргийлэх хөтөлбөр, үйл ажиллагаанд хяналт тавьдаг. Кибер гэмт хэргээс хамгаалах харилцааг Эрүүгийн хууль, Нийгмийн сүлжээн дэх хуулийн хэрэгжилтийг хангах тухай хууль, Иргэний хууль болон Теле мэдээллийн хэрэгслийн тухай хууль зэрэг хуулиудаар тус тус зохицуулж байна.

ИБУИНХУ: Тус улсын Засгийн газраас цахим гэмт хэрэгтэй тэмцэх бодлогын баримт бичгийг 5 жилийн хугацаатай боловсруулан баталдаг бөгөөд 2016-2021 онд “Үндэсний цахим аюулгүй байдлын стратеги”-ийг хэрэгжүүлж, тус бодлогын баримт бичигт хэрэгжилтийн төлөвлөгөөг хавсарган баталсан. Уг стратеги нь цахим аюулгүй байдлыг хангах, урьдчилан сэргийлэх, хөгжүүлэх гэсэн 3 цогц төлөвлөгөөнөөс бүрдэж байна. Найдвартай цахим харилцаа холбоог бий болгох, засгийн газар болон чухал шаардлагатай объектуудын цахим аюулгүй байдлыг хангах, гадаад, дотоодын террорист халдлагаас урьдчилан сэргийлэх, цахим аюулгүй байдлыг хангах байгууллага, нэгжүүдийн техник технологи болон хүний нөөцийн чадавхыг бэхжүүлэх зэрэг ажлуудыг төлөвлөн хэрэгжүүлж байна.

Тус улсын хууль сахиулах байгууллагын цахим гэмт хэрэгтэй тэмцэх нэгжүүд нь зохион байгуулалттай гэмт хэрэгтэй тэмцэх хүрээнд өөр хоорондоо болон бүсийн хэмжээнд олон

https://www.csoonline.com/article/3626908/18-new-cybersecurity-bills-introduced-as-us-congressional-interest-heats-up.html

улсын хууль сахиулах байгууллагууд, тухайлбал, Европол, Холбооны Мөрдөх Товчоо, АНУ-ын Тагнуулын Алба зэрэг байгууллагуудтай хамтран ажилладаг байна. Цахим гэмт хэрэгтэй холбоотой харилцааг олон тооны хууль, тогтоомжоор зохицуулдаг бөгөөд цахим орчны аюулгүй байдлыг хангахад төр, интернэтээр үйлчилгээ үзүүлэгч байгууллагуудын үүрэг, хариуцлага, хяналтын асуудлуудыг нарийвчлан зохицуулсан байна.

БНСУ: 2019 онд Өмнөд Солонгос Улс кибер халдлага, гэмт хэргээс урьдчилан сэргийлсэн Кибер аюулгүй байдлын үндэсний стратегийг боловсруулжээ. Уг стратеги нь 6 зорилтот хөтөлбөртэй байна. Эдгээр зорилтот хөтөлбөрүүд нь үндэсний дэд бүтцийн аюулгүй байдлыг сайжруулах, кибер халдлагад шуурхай хариу арга хэмжээ авах, олон улсын хамтын ажиллагааг хөгжүүлэх, кибер аюулгүй байдлын эрх зүйн орчныг сайжруулах зэрэг арга хэмжээнүүдийг багтаасан байна. БНСУ-д 2015 оноос эхлэн Ерөнхийлөгчид шууд харьяалагддаг Үндэсний аюулгүй байдлын зөвлөл (ҮАБЗ) нь кибер аюулгүй байдалтай холбоотой асуудлуудыг удирдан зохицуулж ирсэн байна.[399] Үндэсний аюулгүй байдлын зөвлөлийн харьяанд байх Цахим аюулгүй байдлын үндэсний төв нь цахим гэмт хэрэг, халдлага аюулгүй байдалтай холбоотой асуудлуудыг хариуцан ажилладаг. Цахим аюулгүй байдлын үндэсний төв нь Шинжлэх ухаан, мэдээлэл, технологийн яам болон Үндэсний Батлан хамгаалах яамтай хамтран хувийн хэвшил болон төрийн байгууллагуудын цахим аюулгүй байдлыг хариуцаж хоорондоо нягт уялдаатай хамтран ажилладаг байна.

МАЛАЙЗ УЛС: Тус улсад 2020-2024 онд хэрэгжүүлэх кибер аюулгүй байдлын төлөвлөлт, хэрэгжилтийн бүх асуудлыг зохицуулах 5 чиглэл бүхий стратеги боловсруулсан байна. Энэхүү кибер аюулгүй байдлын стратеги[400] (Malaysia Cyber Security Strategy)-т үр дүнтэй засаглал, эрх зүйн орчныг сайжруулах, инновац, технологи, судалгааны ажлуудыг түргэсгэх, олон нийтийн мэдлэг боловсролыг дээшлүүлэх, олон улсын хамтын ажиллагааг бэхжүүлэх зэрэг зорилтууд тусгагдсан байна. 1997 онд Компьютерийн гэмт хэрэгтэй тэмцэх тухай хуулийг (The Computer Crimes Act) баталсан ба 2011 оны 12-р сарын 1-нд дахин шинэчилсэн байна.

Түлхүүр үг: *Кибер гэмт хэрэг, кибер халдлага, Кибер аюулгүй байдал, Мэдээллийн аюулгүй байдал, Кибер аюулгүй байдлын индекс, Будапештийн Кибер гэмт хэрэгтэй тэмцэх тухай конвенц*

Keywords: *Cyber crime, Cyber attack, Cyber threat, Cybersecurity, Information security, Global cyber security index, Budapest cybersecurity convention*

[399] From 2015 to 2018, the NSC designated the cybersecurity adviser to lead the cybersecurity efforts nation-wide, however, this position was merged with the cyber information convergence adviser under the same NSC

[400] Malaysia Cyber Security Strategy (2020-2024) https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

Хүснэгт 1. Судалгаанд авагдсан орнуудын онцлох туршлага, эрх зүйн орчны талаарх мэдээллийг доорх хүснэгтээр хураангуйлан танилцуулав.

Улс	Цахим гэмт хэргийн нөхцөл байдал	Кибер гэмт хэрэгтэй тэмцэх стратегитай эсэх	Хэрэгжүүлэгч байгууллагууд	Эрх зүйн орчны лавлагаа
АНУ	Цахим гэмт хэргийн мэдээллийн сүлжээ (Cybertipline) нь 2020 оны байдлаар цахимаар үйлчилгээ эрхлэгчдээс хүүхдийг бэлгийн хүчирхийлэл, садар самуун үйлдэлд ашигласан талаарх 21.7 сая мэдээлэл хүлээн авсан байна.[401] (Дэлгэрэнгүйг судалгааны хэсгээс харах)	-2018 онд батлагдсан “Үндэсний цахим стратеги” (National Cyber Strategy) -2021 онд батлагдсан “Богино хугацааны Үндэсний Аюулгүй байдлын Стратегийн Удирдамж” (Interim National Security Strategic Guidance) -2021 онд гаргасан “Үндэсний Цахим Аюулгүй байдлыг сайжруулах тухай” (Executive Order on Improving the Nation’s Cybersecurity) Ерөнхийлөгчийн зарлиг	-Батлан Хамгаалах Яам (Department of Defense)-ны харьяа Үндэсний Аюулгүй байдлын Агентлаг (National Security Agency) -Дотоодыг Аюулаас хамгаалах Яам (Department of Homeland Security)-ны харьяа Цахим Аюулгүй байдал, Дэд бүтцийн Аюулгүй байдлын Агентлаг (Cybersecurity and Infrastructure Security Agency) -Дотоодыг Аюулаас хамгаалах Яамны харьяа АНУ-ын Тагнуулын газар (US Secret Service) -Хууль зүйн яам (Department of Justice)-ны харьяа агентлаг -Холбооны Мөрдөх Товчоо (Federal Bureau of Investigation)	-Компьютерт хууль бусаар нэвтрэхийг хориглох тухай хууль -Холбооны Мэдээллийн Аюулгүй байдлын Менежментийн тухай хууль -Цахим Харилцаа холбооны Нууцлалын тухай хууль -Цахим Аюулгүй байдлын мэдээлэл солилцох тухай хууль -Цахим ертөнцөд хүүхдийн нууцыг хамгаалах тухай хууль -Интернэт орчинд хүүхдийг хамгаалах тухай хууль -Хүүхэд хамгаалал, аюулгүй байдлын тухай хууль -21-р зуунд хүүхдийг хамгаалах тухай хууль -Домэйн нэр үнэн зөв байх тухай хууль[402] -Цахим гэмт хэргийн мэдээллийн шинэчлэлийн тухай хууль -Ялгаварлан гадуурхах гэмт хэргээс урьдчилан сэргийлэх тухай
Герман Улс	2020 онд Герман Улсад 108,474 кибер гэмт хэрэг бүртгэгдсэн нь 2019 оныхоос 7.9%-иар, 2015 оныхоос 2 дахин нэмэгдсэн байна.	Кибер аюулгүй байдлын стратеги- 2021	-Холбооны Хууль зүйн яам, -Гэр бүлийн яам, -Цагдаагийн байгууллага, -Эрүүгийн цагдаагийн газар хариуцахаас гадна Гэр бүлийн яамны харьяа Хүүхэд, залуучуудад хортой мэдээллийн хяналтын	-Эрүүгийн хууль -Нийгмийн сүлжээн дэх хуулийн хэрэгжилтийг хангах тухай хууль -Теле мэдээллийн тухай хууль -Залуучуудыг хамгаалах тухай хууль

[402] https://www.law.cornell.edu/uscode/text/34/subtitle-II/chapter-209

			холбооны зөвлөл (BPJM), Цахим орчин дахь хүүхэд, залуучуудыг хамгаалах комисс (KJM)	
Япон Улс	2021 оны 3-р сарын байдлаар Үндэсний цагдаагийн газраас явуулсан судалгаагаар 18-аас доош насны 1819 хүүхэд 2020 онд нийгмийн сүлжээтэй холбоотой гэмт хэргийн хохирогч болсон болохыг тогтоожээ.	2021 оны 9 сард Кибер аюулгүй байдлын 3 дахь стратеги төлөвлөгөөг батлан гаргасан байна.	-Цагдаагийн ерөнхий газар, -Ерөнхий газрын “Кибер гэмт хэрэгтэй тэмцэх төв”	-Эрүүгийн хууль, -Интернэтийн аюулгүй орчныг бүрдүүлэх тухай хууль -Зөвшөөрөлгүйгээр цахим сүлжээнд нэвтрэхийг хориглох тухай хууль -Кибер аюулгүй байдлын тухай хууль
Солонгос	2020 оны байдлаар БНСУ-ын цагдаагийн байгууллагад 234 мянга орчим цахим гэмт хэрэг бүртгэгдсэн ба энэ нь өмнөх оноос 54 мянга орчмоор нэмэгдсэн байна.		-Үндэсний тагнуулын албаны дэргэдэх Цахим аюулгүй байдлын үндэсний төв -Шинжлэх ухаан мэдээлэл технологийн яам (Ministry of Science and ICT) -Үндэсний Батлан хамгаалах яам (Ministry of National Defense)	-Эрүүгийн хууль -Сүлжээний тухай хууль Харилцаа холбооны нууцыг хамгаалах тухай хууль -Мэдээлэл, харилцаа холбооны дэд бүтцийг хамгаалах тухай -Цахим засаглалын тухай хууль -Үндэсний батлан хамгаалахын мэдээллийн дэд бүтцийг бий болгох, мэдээллийн нөөцийг удирдах тухай хууль -Зээлийн мэдээллийн ашиглалт, хамгаалалтын тухай хууль (Credit information use and protection act), -Байршлын мэдээллийг хамгаалах тухай хууль -Үйлдвэрлэлийн технологийг хамгаалах тухай хууль -Цахилгаан холбооны бизнесийн болон санхүүгийн луйврын тухай хууль
Малайз	Малайзын цагдаагийн байгууллагын мэдээлснээр 2019 онд кибер халдлага, гэмт хэргийн тоо 3,787	Малайз Улсын кибер аюулгүй байдлын стратеги[404] (Malaysia Cyber Security Strategy)	Үндэсний кибер аюулгүй байдлын агентлаг (NACSA)	-Компьютерийн гэмт хэрэгтэй тэмцэх тухай хууль -Зохиогчийн эрхийн тухай хууль (The copyright (amendment act), -Тоон гарын үсгийн тухай хууль (The digital signature

[404] Malaysia Cyber Security Strategy (2020-2024) https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

	байсан бол 2020 онд 4,194 болж 10%-иар нэмэгдсэн байна. 2021 онд энэ тоо нэмэгдэх төлөвтэй байгаа аж[403].			act), -Телемедициний тухай хууль (The telemedicine act), -Харилцаа холбоо ба мультимедиан тухай хууль (The communications and multimedia act), -Цахим худалдааны тухай хууль(Electronic commerce act), -Төрийн цахим үйл ажиллагааны тухай хууль (Electronic government activities act), -Хувийн мэдээллийг хамгаалах тухай хууль (Personal data protection act), эрүүгийн хууль Penal code), -Хуурамч мэдээллийн эсрэг хууль (The anti-fake news act)
ИБУИНХУ	Цахимаар хамгийн их үйлдэгдэж буй гэмт хэргийн төрлүүдэд дараах хэргүүд ордог байна: Нууц үг ашиглах, хувийн мэдээлэл (phishing), сүлжээнд халдах (malicious software) Мөнгө хулгайлах зорилгоор цахим хуудас руу халдах ингэхдээ тухайн цахим хуудасны сүлжээ болон серверийг хэт их ачааллах замаар үйлдэх (Distributed denial of service).	ИБУИНХУ нь 5 жил тутам “Үндэсний Цахим Аюулгүй байдлын Стратеги” (National Cyber Security Strategy)-ийг шинэчлэн боловсруулж, баталдаг.	-Үндэсний Гэмт хэрэгтэй тэмцэх Агентлаг (National Crime Agency) -Цагдаагийн газар -Бүсийн зохион байгуулалттай гэмт хэрэгтэй тэмцэх нэгжүүд -Үндэсний Цахим Аюулгүй байдлын Төв (National Cyber Security Centre)	-Компьютерийн зүй бус хэрэглээний тухай -Харилцаа холбооны тухай хууль -Хор нөлөөтэй харилцаа холбооны тухай хууль -Дижитал Эдийн засгийн тухай хууль -Айлган сүрдүүлэхээс хамгаалах тухай хууль -Гэмт хэрэгтэнд хариуцлага тооцох ба нийтийн хэв журмыг сахиулах тухай хууль -Боловсрол болон хяналт шалгалтын тухай -Хүүхэд хамгаалын тухай хууль -Бэлгийн хүчирхийлэлтэй тэмцэх тухай хууль

Дэлгэрэнгүй мэдээллийг судалгааны хэсгээс үзнэ үү.

[403] Малайз Улс Кибер гэмт хэргийн нөхцөл байдал The Star Hews https://www.thestar.com.my/news/nation/2021/06/28/cybercrime-increasing-as-more-people-rely-on-digital-tech-during-pandemic-says-pm

СУДАЛГААНЫ ДЭЛГЭРЭНГҮЙ ХЭСЭГ

БҮЛЭГ I. КИБЕР ГЭМТ ХЭРГИЙН ТАЛААРХ ҮНДСЭН ОЙЛГОЛТ

1.1 КИБЕР ГЭМТ ХЭРЭГ, ХАЛДЛАГЫН ТУХАЙ ЕРӨНХИЙ ОЙЛГОЛТ

Интернэтийн хэрэглээ эрс нэмэгдэж, зөвхөн компьютер төдийгүй төрөл бүрийн ухаалаг төхөөрөмж ашиглан сүлжээнд холбогддог болсон, өдөр тутмын амьдралын олон хэрэглээг ухаалаг төхөөрөмж, цахим сүлжээ ашиглан явуулдаг болсонтой зэрэгцэн технологийн ололт амжилтыг гэмт хэрэг үйлдэх зорилгоор ашиглах, үйлдэгдэж байгаа гэмт хэргийн төрөл, хэлбэр, арга, технологи илүү боловсронгуй болох хандлагатай байна.

Цахим орчин дахь гэмт хэргийн тухай ойлголтыг авч үзэхдээ юуны өмнө кибер орон зай, халдлагуудын хэлбэр, тодорхойлолтуудыг сайтар ойлгосон байх шаардлагатай.

Кибер /Cyber/ гэх нэршил нь кибернетик гэх үгтэй утга дүйх ба утгачлан тайлбарлавал нарийн тооцоолон бодох техник-технологийн туслалцаатайгаар мэдээллийг боловсруулах, үйл ажиллагааг удирдах буюу залуур зүй (удирдахуйн тогтолцоо) гэж ойлгогдоно. Европын холбооноос цахим орон зайг нийтэд нь кибер орчин хэмээн тодорхойлж байна.[405]

Кибер гэмт хэрэг гэдэгт кибер халдлага, фишинг, онлайн мөрдлөг, заналхийлэл, скиминг буюу картны гэмт хэрэг, онлайн залилан, садар самуун дүрс бичлэг тараах, интернэтэд суурилсан оюуны өмчийн эсрэг гэмт хэргүүдийг багтаан ойлгодог.[406] Өөрөөр хэлбэл, компьютер, мэдээллийн сүлжээ, интернэт ашиглан үйлдэгдсэн бүх төрлийн гэмт хэргийг хэлнэ.[407]

Цахим хүчирхийлэл гэдэг[408] нь хэн нэгэн этгээд цахим технологийг ашиглан бусад хүнийг дарамтлах, заналхийлэх, ичээх, эсвэл түрэмгийлэх явдал юм. Энэ нь гар утас, компьютер, таблет, тоглоомын систем гэх мэт төхөөрөмж ашиглан үйлдэгддэг.[409]

Мэдээллийн аюулгүй байдал гэдэг нь мэдээлэл болон мэдээллийн системд зөвшөөрөлгүй хандах, мэдээллийг ашиглах, ил болгох, өөрчлөх, хуулах, устгах, мэдээллийн системийн үйл ажиллагааг тасалдуулах, гаднаас хяналт хийхээс хамгаалахыг хэлнэ.[410]

Кибер аюулгүй байдал гэдэг нь кибер гэмт хэргээс систем, сүлжээ, өгөгдлийг хамгаалахад зориулагдсан технологи, үйл явц, арга хэмжээнээс бүрддэг.[411] Кибер аюулгүй байдал нь кибер халдлагын эрсдэлийг бууруулж, систем, сүлжээ, технологийг санаатайгаар ашигласаар байгаа хүмүүсээс аж ахуйн нэгж, байгууллага, хувь хүмүүсийг хамгаалахад чиглэгддэг. Кибер халдлагууд нь олон янзын хэлбэртэй байна. (жишээ нь програмын довтолгоонууд, malware, ransomware, фишинг гэх мэт).

[405] Б.Хишигдорж, Цахим мэдээллийн орчинд үйлдэгдэх гэмт хэргийн мөрдөн шинжлэхүйн онол арга зүйн үндэс сурах бичиг 2015
[406] https://searchsecurity.techtarget.com/definition/cybercrime
[407] Д.Сумъяацэрэн Монгол Улс дахь кибер гэмт хэргийн өнөөгийн байдал, 2016 https://www.slideserve.com/maina/4923860
[408] https://kidshealth.org/en/parents/cyberbullying.html
[409] https://www.verywellfamily.com/types-of-cyberbullying-460549
[410] Мэдээллийн аюулгүй байдлын газар
[411] Төрийн мэдээлэл холбооны газар

Кибер халдлага нь ихэвчлэн хулгайгаар (төлбөрийн картын өгөгдөл, хэрэглэгчийн мэдээлэл, компаний нууцлал, оюуны өмчийн эрхийг зөрчих гэх мэт) сүлжээнд зөвшөөрөлгүй нэвтрэн хохирогч этгээдэд санхүүгийн болон нэр хүндийн хохирол учруулах зорилгоор хийгддэг ажиллагаа юм.

Кибер халдлагууд улам бүр боловсронгуй болсоор байгаа ба олон улсад аливаа улсын засгийн газрын мэдээллийн санд халдаж улс орны аюулгүй байдал, батлан хамгаалах, цэрэг, стратеги, улс төрийн салбарт чиглэсэн аюул занал учруулах явдал түгээмэл болж байна.

1.2 ХАЛДЛАГЫН АРГА ХЭЛБЭРҮҮД

Кибер гэмт хэрэгтний зүгээс халдлага үйлдэх хэд хэдэн арга хэлбэрүүд байдаг ба ерөнхийд нь дараах 3 хэлбэрээр ангилдаг байна.[412]

- Хувь хүний эсрэг чиглэсэн (вирус, залилан,фишинг, спэм г.м)
- Өмчийн эсрэг (бусдын эд хөрөнгийг сүйтгэх, хортой програм тараах г.м)
- Төрийн эсрэг (кибертерроризм, мэдээллийн дайн г.м)

Хувь хүн болон өмчийн эсрэг чиглэсэн: хортой програмыг компьютерт оруулах, эсхүл өгөгдлийг хулгайлах зэрэг олон арга замаар халдлага үйлддэг байна. Үүнд:

- **Social engineering**-Хувь хүний сул талыг ашиглан хортой холбоос дээр даруулах, эсвэл хууран мэхлэх замаар компьютерт нэвтрэх эрх олж авах арга;
- **Phishing /өгөөш хаях замаар хохирогчийг удирдах/**-Хуурамч аж ахуйн нэгж байгуулах, эсхүл тэднийг төлөөлөх замаар хэрэглэгчийн мэдээллийг олж авахыг оролдох үйлдэл;
- **Pharming /Интернэт залилан/-**Вэб сайтын мэдээллийн урсгалыг өөр зүгт чиглүүлэх, хуурамч вэбсайт үйлдэх зэргээр хувь хүний мэдээллийг хулгайлах халдлага;
- **Drive-by /жолоодох/**-Систем доторх тодорхой сул талуудыг ашиглаж халдах;
- **Man in the middle /зуучлагч/**-Талуудын харилцаанд хөндлөнгөөс оролцож үр дүнд нь хакер хоёр талыг хоёуланг нь удирдах, хохироох боломжтой болох арга.

Malware нь компьютерийн системийг тасалдуулах, гэмтээх, зөвшөөрөлгүй нэвтрэх зорилгоор тусгайлан бүтээсэн програм хангамж бөгөөд эдгээр нь дараах хэлбэртэй байдаг:

- **Ransomware** нь компьютерийн систем дээр хортой програмаар кибер халдлагыг эхлүүлсний дараа төлбөр шаарддаг хэлбэр юм. Энэ төрлийн хорт програм нь гэмт хэрэгтнүүдийн дунд түгээмэл болж, жил бүр сая сая байгууллагыг хохироож байна.
- **Viruses** (Вирус) нь нэг компьютерээс нөгөө компьютерт өөрөө өөрийгөө хуулбарлах боломжтой жижиг хэмжээний код юм.
- **Worms** (Өт) нь бусад компьютеруудад тархахын тулд өөрийгөө хуулбарладаг бие даасан хортой програм юм.
- **Trojans** (Троян) вирус нь нэг функц (жишээлбэл, вирус арилгах) мэт харагддаг Програм боловч яг үнэндээ үйлдэл хийх үед системийг гэмтээдэг байна.
- **Spyware/adware** төрөл бүрийн файл хавсаргадаг ба үүнийг нээх холбоос дээр дарах эсвэл хортой програмыг татаж авах үед системд нэвтэрч хохирол учруулдаг.

[412] Д.Сумъяацэрэн, Монгол Улс дахь кибер гэмт хэргийн өнөөгийн байдал, 2016 https://www.slideserve.com/maina/4923860

Төрийн эсрэг чиглэсэн дараах халдлагууд түгээмэл байдаг. Үүнд:

- **Cyber terrorism** нь террорист бүлэглэлүүдээс засгийн газрын үзэл суртлын болон улс төрийн хөтөлбөрт нэвтрэн орж тодорхой зорилгоор мэдээллийн технологийг ашигладаг хэлбэр юм. Сүлжээнүүд, компьютерийн систем, харилцаа холбооны дэд бүтцэд нэвтэрч халддаг.[413]
- **Cyber warfare** нь улс үндэстний сүлжээнд нэвтэрч, мэдээллийн технологийг доголдуулдаг. Cyber warfare довтолгоонууд нь үндсэн сүлжээг эвдэх ба тухайн сүлжээний хэвийн ажиллагааг тасалдуулах чухал өгөгдлийг боогдуулах замаар халдлага үйлддэг.[414]
- **Cyber espionage** нь эзэмшигчийн зөвшөөрөлгүйгээр нууц мэдээллийг олж авах тагнах хэлбэр юм. Cyber espionage нь стратегийн, эдийн засгийн, улс төрийн, цэргийн давуу талыг олж авахад ашиглагддаг.[415]

1.3 ЦАХИМ ОРЧИН ДАХЬ ХҮЧИРХИЙЛЛИЙН ХЭЛБЭР

Цахим хүчирхийллийн хэлбэрийг Монгол Улсын Харилцаа холбооны зохицуулах хорооноос дараах байдлаар авч үзсэн байна. Үүнд:[416]

1. Хэн нэгэн рүү өелдэг бус доромжилсон эсвэл сүрдүүлсэн и-мэйл, чат, текст, мессеж илгээх;
2. Хэн нэгний цахим хаяг, бүртгэлд зөвшөөрөлгүй халдах, ашиглах;
3. Бусдын хувийн зураг, мэдээллийг хуулбарлан байршуулж, эвлүүлэг хийх, бичлэг хийх замаар бусдыг гутгэх доромжлох;
4. Онлайн тоглоом тоглохдоо хэн нэгэнтэй бүдүүлэг, өелдэг бус харьцах;
5. Бусдын хувийн тааламжгүй зургийг цахим орчинд байршуулах, бусдад илгээх, хуваалцах;
6. Хэн нэгнийг элэглэн дуурайсан, хуурч мэхэлсэн нийгмийн сүлжээний хуурамч хаяг үүсгэх, ашиглах;
7. Хэн нэгнийг анги сургууль, олон нийтийн нийгмийн сүлжээний групп, онлайн харилцаанд ямар нэг шалтгаангүйгээр оролцуулахгүй байх, блок хийх зэрэг байна.

Монгол Улсын нийт хүн амын 37.6 хувийг 0-18 хүртэлх насны хүүхэд эзэлж байна. Гэтэл цахим хүчирхийллийн золиос нь насанд хүрээгүй хүн буюу хүүхдүүд болох нь элбэг байна. Манай улсын нийт хүн амын 80.6 хувь нь интернэт хэрэглэгч[417], түүний дотор ухаалаг утастай хүүхдүүдийн 95 хувь нь интернэт хэрэглэдэг, мөн тэдний 92 хувь нь фэйсбүүк хаягтай байгаа[418] нь цахим орчин болон нийгмийн сүлжээнд агуулгын эрсдэл, харилцааны эрсдэл, үйлдлийн эрсдэл гарч болохоор байна.

[413] https://www.nato.int/cps/en/natohq/topics_140739.htm?
[414] https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf
[415] https://www.vmware.com/topics/glossary/content/cyber-espionage
[416] Цахим орчин хүүхэд хамгаалал сэдэвт хэвлэмэл фостерын сан, Харилцаа холбооны зохицуулах хороо http://ekids.mn/Home/newsdetail?dataID=22012&fbclid=IwAR2YroLWF0HURKca5LdAYWTQH5Fr5kGOy5JwOxQlCEOer_x_7CNkqt_QixY
[417] Харилцаа, холбоо, мэдээллийн технологийн газар https://dashboard.cita.gov.mn/
[418] “Өсвөр үе ба цахим хэрэглээ” судалгаа, Гэр бүл, хүүхэд, залуучуудын хөгжлийн газар, 2018 он https://bit.ly/2RlBGNE

БҮЛЭГ II. КИБЕР ГЭМТ ХЭРЭГТЭЙ ТЭМЦЭХ ОЛОН УЛСЫН ЗОХИЦУУЛАЛТ БА НИЙТЛЭГ АСУУДЛУУД

2.1 КИБЕР ГЭМТ ХЭРЭГТЭЙ ТЭМЦЭХ ТУХАЙ БУДАПЕШТИЙН КОНВЕНЦ

Кибер аюулгүй байдлын олон талт хамтын ажиллагааны эрх зүйн үндэс нь Кибер гэмт хэргийн тухай Будапештийн конвенц[419] юм.

Цахим буюу Кибер гэмт хэргийн тухай Будапештийн конвенц нь үндэсний хэмжээний хууль тогтоомжуудыг уялдуулах, мөрдөн байцаах арга техникийг сайжруулах, улс хоорондын хамтын ажиллагааг нэмэгдүүлэх замаар интернэт болон компьютерийн гэмт хэрэг (кибер гэмт хэрэг)-ийг илрүүлэх, таслан зогсоох, шийдвэрлэх зорилготой олон улсын гэрээ юм.

Кибер гэмт хэрэг нь нийгмийн сүлжээ (social network), цахим орчинд үйлдэгддэг. Будапештийн Кибер гэмт хэрэгтэй тэмцэх тухай конвенц нь 2001 оны 11 дүгээр сарын 23-нд батлагдаж 2004 оны 7-р сарын 1-ний өдрөөс хүчин төгөлдөр болсон бөгөөд гишүүн бус улс орнууд ч мөн гарын үсэг зурж нэгдэхэд нээлттэй гэрээ юм.[420] Конвенц нь интернэт орчинд болон компьютерийн бусад сүлжээгээр дамжуулан үйлдэгдсэн зөрчил, ялангуяа зохиогчийн эрх, компьютертэй холбоотой залилан, хүүхдийн садар самуун, сүлжээний аюулгүй байдлыг зөрчсөн гэмт хэрэг зэрэг компьютерийн сүлжээг ашиглан үйлдэгдсэн олон төрлийн зөрчил, гэмт хэргийг таслан зогсоох, нийгмийг кибер гэмт хэргээс хамгаалахад чиглэсэн хууль, эрх зүйн нийтлэг бодлогыг тодорхойлох, ялангуяа улс орнууд зохих хууль тогтоомжийг баталж, олон улсын хамтын ажиллагааг хөгжүүлэхийг дэмжсэн конвенц юм.

Уг конвенцын 2 дугаар бүлгийн 1-10 дугаар заалтад дараах 4 төрлийн үндсэн халдлага, зөрчлийг тодорхойлсон байна.[421]

- Компьютерийн мэдээллийн системийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдлын эсрэг гэмт хэрэг;
- Компьютертэй холбоотой гэмт хэрэг, тухайлбал, залилан, хуурамч баримт бичиг үйлдэх;
- Агуулгатай холбоотой зөрчил-хүүхдийг садар самуунд уруу татах агуулга;
- Зохиогчийн эрхийн зөрчил.

Будапештийн конвенц нь цахим гэмт хэрэгт хариуцлага хүлээлгэх эрх зүйн орчинг бүрдүүлэхээс гадна олон улсын хамтын ажиллагааны үндсийг тодорхойлсон эрх зүйн баримт бичиг юм.[422]

Уг конвенцод нэгдэн орсноор тухайн улс орон конвенцыг дотоодын хууль тогтоомжийн чиглэл болгон ашиглаж болох ба дараах давуу талуудыг бий болгоно.

[419] Кибер гэмт хэргийн тухай конвенц, 2001.11.23 https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[420] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[421] https://statesassembly.gov.je/scrutinyreviewresearches/2018/research%20-%20briefing%20paper%20on%20council%20of%20europe%20convention%20on%20cybercrime%20-%2031%20october%202018.pdf

[422] https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac#:~:text=The%20Budapest%20Convention%20requires%20States,cybercrime%20but%20any%20offence%20where

- Олон улсын хамтын ажиллагааны эрх зүйн үндэс бүрдэнэ.
- Нэгдэн орсон талууд цаашид конвенцын хөгжилд нэмэлт санал, протокол оруулж болно.
- Конвенцод нэгдсэн орнууд энэхүү гэрээний дагуу байгуулагдсан цэгүүдтэй 24 цагийн холболттой байна.
- Талууд хувийн хэвшилтэй хамтын ажиллагаагаа хөгжүүлж туршлагажих боломжтой.
- Оролцогч талууд өөрийн хүсэл санаачилгаар чадавхыг бэхжүүлэхэд тэргүүлэх үүрэг рольтой төв болж болно.

Будапештийн конвенцтой уялдуулан дотоодын хууль эрх зүйн орчныг бий болгосноор олон улсын цахим гэмт хэрэгтэй тэмцэх шалгуурыг хангах нөхцөл бүрдэх юм. Энэхүү конвенц нь олон улсын хамтын ажиллагааг сайжруулахаас гадна олон улсад тавигдаж буй хууль эрх зүйн шаардлагыг хангахад тусалдаг. Конвенцын талаарх зарим мэдээллийг Хавсралт 3-аас үзнэ үү.

2.2 КИБЕР АЮУЛГҮЙ БАЙДЛЫН ОЛОН УЛСЫН СТАНДАРТ

Олон улсын стандартчиллын байгууллагаас (ISO) кибер аюулгүй байдлын ойлголт, шалгуур, боловсронгуй болгох зарчмуудыг багтаасан *ISO/IEC 27032:2012 Information technology буюу* Олон Улсын *Мэдээллийн технологийн* стандартыг 2012 оны 7 дугаар сард баталсан байна.[423] Уг стандартад кибер аюулгүй байдал, сүлжээний аюулгүй байдал, хэрэглээний аюулгүй байдал, интернэтийн аюулгүй байдал, дэд бүтцийн аюулгүй байдал гэх мэт нэр томьёонуудыг тодорхойлсон байна. Түүнчлэн ISO 27001 стандарт гэж байх ба энэ нь мэдээллийн аюулгүй байдлын менежментийн олон улсад хүлээн зөвшөөрөгдсөн стандарт юм. Энэхүү стандартыг хэрэгжүүлснээр мэдээллийг хамгаалах, мэдээллийн аюулгүй байдлыг хангахтай холбоотой арга хэмжээнүүдийн шалгуур үзүүлэлтийг тодорхойлж, талуудад баталгаа өгдөг байна.

2.3 ДЭЛХИЙН КИБЕР АЮУЛГҮЙ БАЙДЛЫН ИНДЕКС (GCI)

Америк, Англи, Герман тэргүүтэй өрнөдийн хөгжингүй орнууд кибер аюулгүй байдлаараа дэлхийд тэргүүлж байна. Цахим халдлагаас өөрийгөө хамгаалах чадамжийг Олон улсын харилцаа холбооны байгууллага *(International Telecommunication Union)*-аас гаргасан “Дэлхийн кибер аюулгүй байдлын индекс”-ээр (The Global Cybersecurity Index) тодорхойлдог. Уг индекс (GCI) нь дэлхийн улс орнуудын кибер аюулгүй байдлын түвшинг тодорхойлох итгэмжлэгдсэн лавлагаа болдог байна.[424]

Кибер аюулгүй байдал нь олон салбарын огтлолцолд оршдог тул улс орнуудын кибер аюулгүй байдлын хөгжлийн түвшинг дараах 5 үндсэн чиглэлээр үнэлдэг байна.

- Хууль эрх зүйн орчин (Legislative environment)
- Техникийн арга хэмжээ (Technical Measures)
- Байгууллагын арга хэмжээ (Organization Measures)
- Чадавх хөгжүүлэх арга хэмжээ (Capacity Building Measures)
- Хамтын ажиллагаа (Cooperation Measures)

[423] https://www.iso.org/standard/44375.html
[424] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Эдгээр үнэлгээний чиглэл тус бүрт тухайн орны кибер аюулгүй байдлын түвшинг үнэлэх тодорхой шалгуур үзүүлэлтүүд багтдаг байна. Үүнд:[425]

Хууль эрх зүйн орчин

- Кибер аюулгүй байдлын тухай хууль
- Кибер аюулгүй байдлыг зохицуулах арга хэмжээ
- Спам, халдлагыг хязгаарлах хууль эрх зүй

Техникийн арга хэмжээ

- CIRT-(Computer Incident Response Team) Компьютерийн гэмтлийн хариу арга хэмжээний баг
- CERT-(Computer Emergency Response Team) Компьютерийн түргэн тусламжийн баг
- CSIRT-(Computer Security Incident Response Team) Компьютерийн аюулгүй байдлыг хангах хариу арга хэмжээний баг
- Стандарт хэрэгжүүлэх стратеги
- Стандартчиллын байгууллага
- Спам халдлагыг арилгахад чиглэсэн техникийн механизм, чадавх
- Кибер аюулгүй байдлын зорилгод үүлэн технологи ашиглах
- Хүүхэд багачуудыг онлайнаар хамгаалах механизм

Байгууллагын арга хэмжээ

- Үндэсний кибер аюулгүй байдлын стратеги
- Кибер аюулгүй байдлын агентлаг
- Кибер аюулгүй байдлын хэмжигдэхүүн (Cybersecurity metrics)

Чадавх бэхжүүлэх

- Олон нийтийг мэдээллээр хангах
- Кибер аюулгүй байдлын мэргэжилтнийг гэрчилгээжүүлэх, магадлан итгэмжлэх тогтолцоо
- Кибер аюулгүй байдлын талаар мэргэжилтэн бэлтгэх
- Кибер аюулгүй байдлын боловсролын тухай мэргэжлийн багшийн сургалт
- Кибер аюулгүй байдлын эрдэм шинжилгээ, судалгааны хөтөлбөр (цахим дэд бүтцийг хамгаалах хөтөлбөр)
- Урамшууллын механизм

Хамтын ажиллагаа

- Хоёр тал хүлээн зөвшөөрсөн байх;
- Олон тал хүлээн зөвшөөрсөн байх;
- Олон улсын оролцогч талуудтай байх;
- Олон нийтийн болон хувийн хэвшлийн оролцогч талуудтай байх;
- Хамтрагч агентлагуудтай байх;
- Сайн туршлага, үйл ажиллагаатай байх.

[425] https://www.secureworldexpo.com/industry-news/countries-dedicated-to-cybersecurity

Олон улсын харилцаа холбооны байгууллагаас дээрх 5 чиглэлээр шалгуур үзүүлэлтүүдийг үнэлж, индексийг тодорхойлсноор тухайн улс кибер халдлагаас урьдчилан сэргийлэх чадамжтай эсэхийг тодорхойлох ба бодлогын түвшинд дээрх шалгууруудыг тогтоохыг зөвлөмж болгодог байна.

2.4 ОЛОН УЛСЫН КИБЕР АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО

Сүүлийн жилүүдэд кибер аюулгүй байдлыг хангах бодлого, эрх зүйн орчныг бүрдүүлэхээр дэлхийн бүх засгийн газрууд хичээн ажиллаж байна. Жил бүр кибер гэмт хэрэг дэлхийн эдийн засгаас хэдэн зуун тэрбум долларыг залилж, бизнесийн үйл ажиллагааг тасалдуулж, инновацийг саатуулж, ажлын байрны өсөлтийг царцааж байна.[426]

BSA |Олон Улсын Програм хангамжийн холбоо (www.bsa.org) нь дэлхийн засгийн газрууд болон олон улсын зах зээл дээрх програм хангамжийн компаниудыг нэгтгэсэн олон улсын байгууллага юм. Уг байгууллага нь АНУ-ын Вашингтон хотод төвтэй бөгөөд дэлхийн 60 гаруй оронд үйл ажиллагаа явуулдаг. BSA нь хууль ёсны програм хангамжийг сурталчлах, технологийн шинэчлэлийг дэмжих төрийн бодлогыг сурталчлах, олон улсын кибер аюулгүй байдлын бодлогын хүрээнд цахим аюулгүй байдлын цогц шийдлүүдийг санал болгох үндсэн зорилготой.

BSA-ийн гаргасан Бодлогын хүрээ (Policy framework)-нд засгийн газраас кибер аюулгүй байдлын бодлого хэрэгжүүлэхдээ дараах үндсэн 6 зарчмыг баримтлахыг зөвлөж байна.

- Бодлогыг олон улсын хэмжээнд хүлээн зөвшөөрөгдсөн техникийн стандартад нийцүүлэх;
- Бодлого нь эрсдэлд суурилсан, үр дүнд чиглэсэн, төвийг сахисан технологитой байх;
- Бодлого нь зах зээлийн механизмд суурилсан байх;
- Бодлого нь инновацийг дэмжих уян хатан, дасан зохицох чадвартай байх;
- Төр, хувийн хэвшил хосолсон хамтын ажиллагаанд суурилах;
- Бодлого нь хувийн нууцыг хамгаалахад чиглэсэн байх.

Үндэсний кибер аюулгүй байдлын үндсэн элементүүд (BSA):

ЗАСГИЙН ГАЗРЫН ҮЙЛ АЖИЛЛАГААНЫ СТРАТЕГИ

- Кибер аюулгүй байдлын асуудал эрхэлсэн үндэсний байгууллагатай байх;
- Оролцогч талуудын үүрэг, хариуцлагыг тодорхой болгох;
- Байгууллага хоорондын уялдааг бий болгох;
- Үндэсний кибер аюулгүй байдлын стратеги боловсруулах;
- Кибер аюулгүй байдлын дэд бүтцийг бий болгох;
- Үндэсний кибер аюулгүй байдлын төлөвлөгөө, дэд бүтцийг байнга шинэчлэх;
- Салбарын нарийн төлөвлөгөө гаргах;
- Төр болон хувийн хэвшлийн хамтын ажиллагаа оролцоог дэмжсэн бүтэц бий болгох;
- Засгийн газар болон холбогдох байгууллагуудын хамтын ажиллагааны механизмыг бий болгох.

[426] BSA International Cybersecurity Policy Framwork 2018

КИБЕР АЮУЛГҮЙ БАЙДАЛ БА ЗАСГИЙН ГАЗАР

- Үндэсний кибер аюулгүй байдлын яаралтай хариу арга хэмжээний баг бий болгох;
- Цаг тухайд мэдээлэл солилцох, түүнийг дэмжих;
- Халдлагын талаарх мэдээллийн дэд бүтэц бий болгох;
- Хувийн мэдээлэлд халдахад мэдэгдэх стандартыг тогтоох;
- Засгийн газрын үйл ажиллагаа ил тод, сул талуудаа засдаг байх.

ЗАСГИЙН ГАЗРЫН ХАНГАМЖ ҮЙЛЧИЛГЭЭ

- Техник төхөөрөмж худалдан авахдаа төвийг сахих;
- Лицензтэй Програм хангамж ашиглах;
- Програм хангамжийг борлуулагчаар баталгаажуулсан эсэхийг шалгах;
- Үүлэн үйлчилгээний (Cloud service) аюулгүй байдлын давуу талыг ашиглах;
- Техник, төхөөрөмж худалдан авахдаа аюулгүй байдлыг хангах, шалгах;
- Мэдээллийн технологийн системийг ухаалаг, аюулгүй байдлаар удирдах.

ЭРДЭМ ШИНЖИЛГЭЭ, СУДАЛГАА

- Кибер аюулгүй байдлын технологи, төхөөрөмж хэрэгслийн судалгаа, хөгжүүлэлтийг дэмжих.

КИБЕР АЮУЛГҮЙ БАЙДАЛ БА ХУВИЙН ХЭВШИЛ

- Кибер аюулгүй байдлын үр дүнд төвлөрөх;
- Эрсдэлд суурилсан, уян хатан бодлоготой байх;
- Дотоодын стандартаас гадна кибер аюулгүй байдлын дэд бүтцийг олон улсад хүлээн зөвшөөрөгдсөн стандарттай уялдуулах;
- Тэнцвэртэй, ил тод, олон улсын туршлагад суурилсан байх;
- Эх код, бусад оюуны өмчийг нууцлах;
- Бүтээгдэхүүн сонгохдоо зах зээлд суурилсан шийдлүүдийг ашиглах;
- Олон улсын дата ашиглах.
- Шинээр гарч ирж буй технологийг идэвхжүүлэх бодлогын орчинтой байх

КИБЕР АЮУЛГҮЙ БАЙДАЛ БА ИРГЭН

- Кибер аюулгүй байдлын талаар олон нийтэд сурталчлах;
- Хэрэглэгчийн сонголтыг бүртгэх, мэдээлэх хэрэгсэл бий болгох;
- Боловсролын бүх түвшинд цахим аюулгүй байдлын мэдлэгийг суулгах;
- Кибер аюулгүй байдлын талаар боловсрол олгох сургалт зохион байгуулах;
- Кибер аюулгүй байдлын мэргэжилтнүүдийг олон талаар дэмжих.

КИБЕР ГЭМТ ХЭРЭГ

- Кибер гэмт хэрэгтэй тэмцэх тухай Будапештийн конвенцод нийцсэн цогц хууль эрх зүйн орчныг бий болгох;
- Зөвхөн кибер халдлагад чиглэсэн тусгайлсан хууль эрх зүйн зохицуулалттай байх;
- Хууль сахиулах, хэрэгжүүлэгч байгууллагуудад техникийн сургалт, дэмжлэг үзүүлэх.

ОЛОН УЛСЫН ОРОЛЦОО

1. Кибер аюулгүй байдлын хамтын ажиллагааны гадаад бодлогод нэгдэх;
2. Олон улсын хамтын ажиллагаанд хамрагдах;

3. Экспортын хяналтын бодлогыг кибер аюулгүй байдлын хууль ёсны үйл ажиллагаанаас тусад нь авч үзэх;
4. Өөрийн орны нутаг дэвсгэрийг олон улсын кибер халдлагад ашиглахаас урьдчилан сэргийлэх;
5. Хувийн мэдээллийг хамгаалах, хүний эрхийг хамгаалах.

2.5 ЦАХИМ ОРЧИН ДАХЬ ХҮНИЙ ЭРХИЙН ТҮГЭЭМЭЛ ТУНХАГЛАЛ

1948 онд НҮБ-ын Ерөнхий Ассамблейгаас Хүний эрхийн түгээмэл тунхаглалыг баталсан. Тэгвэл өнөөдөр улам бүр даяаршиж байгаа цахим ертөнцөд тэдгээрийн харилцааг зохицуулах, тунхаглах шаардлага тулгарсан. Энэхүү тунхаглалын цахим орчин дахь хувилбар(төсөл)[427]-ыг Роберт Б.Геман хэмээх судлаач боловсруулжээ.

1. Хүн бүр хүний өөрийн санаа бодол, илэрхийллийг шууд ба шууд бусаар илэрхийлэх, түгээх, бусадтай хуваалцах зохих ёсны, тэгш боломжоор хангагдсан байна.
2. Хүн бүр энэхүү тунхаглалд заасан бүх эрх, эрх чөлөөг үндэс угсаа, арьсны өнгө, хүйс, хэл соёл, шашин шүтлэг, үзэл бодол, нийгмийн гарал үүсэл, хөрөнгө чинээ, нийгмийн байдал зэрэг дурын ялгаваргүйгээр тэгш эдэлнэ.
3. Хүн бүр өөрийн хувийн цахим орон зай, нэртэй байж нэр, онлайн хэлцлээ нууцлан хамгаалах эрхтэй.
4. Интернэтийн үйлчилгээ үзүүлэгч байгууллага, вэб сайтаас хүний хувийн мэдээллийг албадан гаргаж өгөхийг шаардаж болохгүй. Шаардлагатай үед зохих зөвшөөрлийн үндсэн дээр мэдээллийг гаргаж өгч болно.
5. Хэн ч урьдчилсан зөвшөөрөл авалгүйгээр сайн дураар нийтэд хандсан их хэмжээний цахим шуудан, сервер компьютерт ачаалал үүсгэх хавсралт файл, хөнөөлт Програм хангамжуудыг илгээх эрхгүй.
6. Хүн бүр интернэтээс мэдээлэл хайх, хүлээн авах эрхтэй. Гагцхүү энэхүү эрхээ эдлэхдээ тухайн харилцаанд тогтоосон зан үйлийн хэм хэмжээг даган мөрдөнө.
7. Цахим ба бодит орон зайд цөөнхийн болон хэрэглэгчийг тусгайлан хамгаална. Газарзүйн харьяаллын гэрээ ёсоор ял оногдуулах тохиолдолд оршин байгаа газрын эрх зүйн тогтолцооноос үл хамааран хувь хүний суурь эрхийг хүндэтгэнэ.
8. Хүн бүр өөрийнх нь эрх, эрх чөлөө зөрчигдөх, хувийн мэдээллээ хортойгоор ашиглуулахын эсрэг хууль зүйн хамгаалалтад байх эрхтэй.
9. Агуулга, онлайн харилцаатай холбогдуулан хэнийг ч дур зоргоор хянаж, шалгахыг хориглоно.
10. Хүн бүр эрх, үүргээ тодорхойлуулах, түүний эсрэг ял тулгасан тохиолдолд ялын үндэслэлийг тогтоолгохоор хараат бус, шударга шүүхээр хууль ёсны, нээлттэй дэгээр шүүлгэх бүрэн эрхтэй.
11. Хүн бүр төрийн байгууллага, интернэтийн үйлчилгээ үзүүлэгчээр дамжуулан хуулиар тусгайлан нууцалснаас бусад мэдээлэлд хандах эрхтэй.
12. Хүн бүр өөрийн харилцаа холбоо, хэлцлээ хамгаалах технологийг сонгох эрхтэй ба энэ эрхийг хэрэгжүүлэхэд нь технологид харшлахыг хориглоно.
13. Хүн бүр өөрийн үзэл бодлоо чөлөөтэй илэрхийлэх эрхтэй. Энэхүү эрх нь итгэл үнэмшил, сүсэг бишрэлээ төрөл бүрийн зан үйлээр илэрхийлэх эрхийг мөн агуулна.

[427] Цахим орчин дахь Хүний эрхийн түгээмэл тунхаглал, http://www.be-in.com/10/rightsdec.html

Хэний ч үзэл бодлоо илэрхийлсэн зан үйлийн хэлбэрт нь ял, зэмлэл хүлээлгэхийг хориглоно.

14. Хүн бүр интернэтийн үйлчилгээ үзүүлэгчийг чөлөөтэй сонгох, түүнийгээ солих эрхтэй. Мөн үйлчилгээний төлбөртэй холбоотойгоор байрлал үл харгалзан “үнэгүй”, “нийтийн” үйлчилгээг сонгох эрхтэй.
15. Хэний ч хандалтын эрх буюу цахим шуудангийн бүртгэлийг үйлчилгээний гэнэтийн өөрчлөлт зэрэг зохисгүй шалтгаан, дур зоргоор хаах, устгахыг хориглоно.
16. Хүн бүр өөртэйгөө онлайнаар холбогдох этгээдээ чөлөөтэй сонгох эрхтэй. Хэнийг ч тодорхой бүлэгт хамруулах, вэб сайтад зочлуулахаар албадахыг хориглоно.
17. Хэн бүхний хувийн мэдээлэл, онлайн үйл ажиллагаа нь хувийн өмч бөгөөд түүнийг тухайн этгээд өөрөө хянана. Хүн бүр энэхүү өмчөө үнэлэх, ил тод болгох, бусадтай солилцох эсэхээ өөрөө шийдэх эрхтэй.
18. Хүн бүр ашиг сонирхол, үнэт зүйл, чиг үүргийн бүлгийг үүсгэх эрхтэй.
19. Хүн бүр шинэ технологийг эзэмших эрхтэй. Төрийн байгууллагаас бүх нийтэд хэрэглээний програм хангамжууд ба онлайн харилцааны сургалтуудыг явуулах үүрэгтэй. Амьдралын хүнд нөхцөлд байгаа хүмүүс, өндөр настангууд болон хэрэгцээт хүмүүст зориулсан сургалт тусгай хөтөлбөрүүдийг авч үзнэ. Сургалт нь хувь хүнд чиглэсэн, тэдний өөрийгөө хүндлэх хүндлэлийг бэхжүүлж, бие даасан байдлыг дэмжихэд чиглэнэ.
20. Эцэг, эхчүүд өөрийн үзэл бодлоор үр хүүхдийнхээ онлайн харилцааг удирдан чиглүүлэх эрх, үүрэгтэй. Энэ асуудлаар ямар ч байгууллага эцэг, эхийн сонголтыг үгүйсгэх эрхгүй.
21. Хүн бүр зохиогчийн эрхээр хамгаалагдах утга зохиол, урлагийн болон шинжлэх ухааны бүтээлээ бусадтай онлайнаар хуваалцах эрхтэй.
22. Хүн бүр энэхүү тунхаглалд заасан эрх, үүргийг хэрэгжүүлэн хувьдаа ашиг, орлоготой болох эрхтэй.
23. Хүн бүр өөрийн зан үйл, илэрхийллээ хариуцах, өөрийн байр суурьтай байх эрхтэй.
24. Энэхүү тунхаглалын зарчмуудыг аль нэг улс орон, бүлэглэл, бие хүний зүгээс энд тунхагласан эрх, эрх чөлөөг үгүйсгэхэд чиглэсэн аливаа үйл ажиллагааг авч хэрэгжүүлэх, агуулгыг мушгин өөрчлөх, өөрчлөн хэрэглэхийг хориглоно.

БҮЛЭГ III. МОНГОЛ УЛСЫН КИБЕР АЮУЛГҮЙ БАЙДЛЫН ЭРХ ЗҮЙН ОРЧИН

3.1 МОНГОЛ УЛС ДАХЬ КИБЕР АЮУЛГҮЙ БАЙДАЛ

Монгол Улсын төр, засгаас харилцаа холбооны салбарыг хөгжүүлэх нь улс орны аюулгүй байдлыг хангахад чухал ач холбогдолтой гэдгийг онцгойлон анхаарч 1922 оноос эхлэн Дотоодыг хамгаалах газрын бүтцэд Шуудан, телефон, радио, шифр холбооны нэгжийг байгуулж ирсэн нь Мэдээллийн аюулгүй байдлын алба үүсэх эх суурь болсон. Техник технологи хурдтай хөгжиж буй өнөөгийн нийгэмд мэдээллийн аюулгүй байдлын асуудал хурцаар тавигдаж байна.

Монгол Улсын Үндэсний аюулгүй байдлын үзэл баримтлал, Тагнуулын байгууллагын тухай хуулийн 11.1.6, Харилцаа холбооны тухай хуулийн 20.3-т төрийн байгууллагуудыг кибер халдлагаас хамгаалах тогтолцоог бүрдүүлэхийг заасан бөгөөд энэ чиг үүргийг Мэдээллийн аюулгүй байдлын газар хэрэгжүүлэн ажиллаж байна.[428]

[428] http://isd.gov.mn/

Тус байгууллага нь төрийн мэдээлэл, харилцаа холбооны аюулгүй байдлыг хангах чиг үүргийн хүрээнд:

1. Төрийн болон онц чухал мэдээллийн сүлжээ, харилцаа холбооны аюулгүй байдлыг хангах, цахим аюул, заналтай тэмцэх;
2. Кибер аюулгүй байдлын талаар баримтлах бодлогын баримт бичгийг боловсруулах;
3. Төрийн байгууллагуудад кибер аюулгүй байдал, мэдээллийн аюулгүй байдалтай холбоотой эрсдлийн үнэлгээ хийх;
4. Кибер аюулгүй байдлын талаар сургалт сурталчилгаа зохион байгуулах;
5. Төрийн болон нутгийн өөрөө удирдах байгууллагын хэрэгцээнд ашиглагдах тусгай хэрэглээний шуудангийн үйлчилгээ үзүүлэх;
6. Төрийн болон төрийн захиргааны байгууллагуудын хооронд төрийн нууц мэдээ, мэдээлэл дамжуулах, солилцох үеийн нууцлал аюулгүй байдлыг хангах гэсэн чиглэлээр үйл ажиллагаагаа явуулж байна.

3.2 МОНГОЛ УЛСЫН ҮНДЭСНИЙ АЮУЛГҮЙ БАЙДЛЫН ҮЗЭЛ БАРИМТЛАЛ

Монгол Улсын Үндэсний Аюулгүй Байдлын Үзэл Баримтлалд мэдээллийн аюулгүй байдлын талаар баримтлах бодлогыг дараах байдлаар тодорхойлсон байдаг.

Мэдээллийн аюулгүй байдал

Мэдээллийн салбарт үндэсний ашиг сонирхлыг хамгаалах, төр, иргэн, хувийн хэвшлийн мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдлыг баталгаажуулах нь мэдээллийн аюулгүй байдлыг хангах үндэс мөн.

3.6.1.Мэдээллийн салбарт үндэсний ашиг сонирхлыг хамгаалах

3.6.1.1.Үндэсний аюулгүй байдлыг хангах, улс орны хөгжлийг дэмжих, үндэсний үнэт зүйлийг хэвшүүлэх, нийгмийн оюун санааг төлөвшүүлэхэд мэдээлэл, мэдээллийн аюулгүй байдал нэн чухал ач холбогдолтой.

3.6.1.2.Нийгмийн сэтгэл зүй, тогтвортой байдал, хувь хүний ухамсар, ёс зүйд хөндлөнгөөс нөлөөлөх оролдлогыг хязгаарлана. Дайсагнал, ялгаварлан гадуурхах үзэл, үзэн ядалтыг сурталчилсан, дэмжсэн сурталчилгаа, мэдээллийг таслан зогсоох, саармагжуулах чадавхыг бий болгож, үл зөвшөөрөх сэтгэхүйг нийгэмд төлөвшүүлнэ.

3.6.1.3.Үндэсний мэдээллийн дэд бүтцэд халдах аюулаас хамгаалах, эдийн засаг, нийгмийн чадавхыг сулруулах оролдлоготой тэмцэх чадавхыг бий болгоно.

3.6.1.4.Монгол Улсад гадаадын хөрөнгө оруулалттай хэвлэл мэдээллийн хэрэгсэл үндэсний аюулгүй байдалд харшилсан үйл ажиллагаа явуулбал үйл ажиллагаа явуулах эрхийг нь хязгаарлаж болно. Хэвлэл мэдээллийн хэрэгслийн эзэмшил, харьяалал нь ил тод байх бөгөөд үйл ажиллагаа нь бодитой, тэнцвэртэй, хариуцлагатай байна. Мэдээллийн хэрэгслээр үндэсний үнэт зүйлийг түлхүү нийтлэх, сурталчлахыг дэмжиж, гадны шашин, соёл, төрийн бодлогыг сурталчилсан агуулгатай мэдээллийг зохистой түвшинд хязгаарлана.

3.6.1.5.Мэдээллийн аюулгүй байдлын үндэсний хэмжээний бодлого, эрх зүйн зохицуулалт, стандарт, удирдлага, зохион байгуулалт, сургалтын тогтолцоог бий болгож нийгэм дэх ойлголт, мэдлэгийг төлөвшүүлнэ.

3.6.1.7.Төр, хувийн хэвшлийн байгууллагад мэдээллийн аюулгүй байдлын бодлого, дэг, эрсдэлийн удирдлага, дотоод аудит, үнэлгээний чадавхыг бий болгоно.

3.6.1.8.Мэдээллийн аюулгүй байдлын орчин үеийн дэвшилтэт, өртөг багатай шийдлийг зөвхөн эрсдэлийн үнэлгээний үндсэн дээр сонгон ашиглана. Төрийн байгууллага, онц чухал дэд бүтцийн объектын мэдээллийн аюулгүй байдлыг хангах чиг үүргийг өндөр түвшинд бэлтгэгдэж, итгэмжлэгдсэн үндэсний мэргэжилтнээр гүйцэтгүүлнэ.

3.6.1.9.Өрсөлдөх чадвартай мэдээлэл, харилцаа холбооны систем, техник хэрэгсэл, програм хангамжийн үндэсний үйлдвэрлэл болон мэдээллийн аюулгүй байдлын шийдэл боловсруулах ажиллагааг дэмжин хөгжүүлж технологийн хараат байдлыг бууруулна.

3.6.1.10.Мэдээлэл, харилцаа холбооны технологи, мэдээллийн аюулгүй байдлын чиглэлээр үндэсний суурь болон хавсарга судалгаа, шинжилгээ, сургалтыг онцгойлон дэмжинэ.

3.6.1.11.Кибер орчин дахь гэмт явдалтай тэмцэх, аливаа гэмт хэргийг илрүүлэх, нотлоход тооцоолох хэрэгслийн криминалистик техникийн шинжилгээ ашиглах үндэсний чадавхыг бий болгоно.

3.6.1.12.Мэдээллийн аюулгүй байдлыг хангах, мэдээллийн орчинд сөргөлдөх аюулаас сэргийлэх, кибер орчин дахь гэмт явдалтай тэмцэх чиглэлд олон улсын хамтын ажиллагааг өргөжүүлэн хөгжүүлнэ.

3.3 ТАГНУУЛЫН БАЙГУУЛЛАГЫН ТУХАЙ ХУУЛЬ

11 дүгээр зүйл.Тагнуулын ерөнхий газрын үүрэг

11.1.Тагнуулын ерөнхий газар дараах үүрэг гүйцэтгэнэ:

11.1.6.Төрийн болон онц чухал мэдээллийн сүлжээ, харилцаа холбооны аюулгүй байдлыг хангах, цахим аюул, заналтай тэмцэх; */Энэ заалтад 2011 оны 6 дугаар сарын 10-ны өдрийн хуулиар өөрчлөлт, 2015 оны 7 дугаар сарын 9-ний өдрийн хуулиар өөрчлөн найруулсан./*

3.4 ХАРИЛЦАА ХОЛБООНЫ ТУХАЙ ХУУЛЬ

20 дугаар зүйл.Тусгай хэрэглээний холбооны сүлжээ

20.1.Монгол Улсын батлан хамгаалах, аюулгүй байдлыг хангах, гамшгаас хамгаалах, гэмт хэрэгтэй тэмцэх, нийгмийн хэв журам сахиулах, төрийн болон нутгийн удирдлагын байгууллагын хэрэгцээнд зориулан тусгай хэрэглээний холбооны сүлжээг байгуулан ажиллуулж болно. */Энэ хэсэгт 2019 оны 05 дугаар сарын 30-ны өдрийн хуулиар өөрчлөлт оруулсан./*

20.2.Тусгай хэрэглээний холбооны сүлжээ төрийн хамгаалалтад байна.

20.3.Тусгай хэрэглээний холбооны сүлжээ байгуулах, ашиглах журмыг Засгийн газар тогтооно.

20.4.Тусгай хэрэглээний холбооны сүлжээнд цахилгаан холбооны суваг, тоног төхөөрөмжийг үйлчлэгчтэй байгуулсан гэрээний үндсэн дээр ашиглана.

20.5.Харилцаа холбооны сүлжээгээр дамжуулах тусгай хэрэглээний холбооны мэдээллийн нууцлалт, хамгаалалтыг энэ хуулийн 20.1-д заасан байгууллага хариуцна.

БҮЛЭГ IV. ГАДААДЫН ЗАРИМ ОРНЫ КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ БОДЛОГО, ЭРХ ЗҮЙН ОРЧИН

4.1 АМЕРИКИЙН НЭГДСЭН УЛС

I. Цахим орчин дахь гэмт хэргийн нөхцөл байдал

АНУ-д цахим гэмт хэрэгтэй тэмцэх ажил 1980-аад оноос эхэлсэн бөгөөд түүнд тавих хяналт, цахим гэмт хэргээс урьдчилан сэргийлэх алхмууд, цахим орчныг зохицуулах эрх зүйн зохицуулалтууд нь гэмт хэргийн гаралт, төрлөөс хамааран боловсронгуй болсоор байна. 2020 оны байдлаар Интернэт гэмт хэргийн талаар гомдол хүлээн авах төвд бүртгэгдсэн цахим гэмт хэргийн төрөлд хувь хүний кредит картны дугаар, картны нууц дугаарыг мэхлэн авах (phishing) болон үүнтэй ижил төрлийн залилангийн хэргүүд хамгийн их бүртгэгдсэн байна.[429] Цахим аюулгүй байдлыг хангах, ард иргэд, улс орны аюулгүй байдлыг хамгаалах, цахим гэмт хэргээс урьдчилан сэргийлэх, цахим гэмт хэрэгтэй тэмцэх асуудлыг Холбооны Засгийн газрын харьяа агентлагууд, хувийн хэвшил болон олон нийтийн байгууллагууд нэгдэн, хамтран хэрэгжүүлж байна.

II. Цахим орчин дахь гэмт хэргийн стратеги төлөвлөгөө

Цахим орчин нь ард иргэдийн өдөр тутмын амьдралд төдийгүй эдийн засаг, батлан хамгаалах зэрэг улс орны амин чухал салбаруудын аюулгүй байдалтай салшгүй холбоотой. Техник технологийн дэвшлийг дагаад цахим халдлага, гэмт хэрэг улам нарийсч, давтамж нь нэмэгдсээр байгаа тул үүнтэй тэмцэх зорилгоор бодлогын баримт бичгүүдийг боловсруулан хэрэгжүүлж байна.

- 2018 онд Ерөнхийлөгч Доналд Трамп **“Үндэсний цахим стратеги”** (National Cyber Strategy)-ийг шинэчлэн баталсан.[430] Стратеги нь дөрвөн үндсэн хэсгээс бүрдэж байна.

Нэгдүгээр хэсэг: Эх орон, ард түмэн, Америк амьдралын хэв маягийг хамгаалах (Америкчуудын амар тайван амьдралыг хамгаалах)

- Холбооны засгийн газрын сүлжээ ба мэдээллийн аюулгүй байдлыг хангах;
- Улс орны чухал дэд бүтцүүдийн аюулгүй байдлыг хангах;
- Цахим гэмт хэрэгтэй тэмцэн, гэмт хэргийг мэдээлэх ажлыг сайжруулах;
- (Цахим тандалт, компьютерээр үйлдэгдэж буй гэмт хэргийн талаарх хуулийг шинэчлэх).

Хоёрдугаар хэсэг: Америкийн хөгжил цэцэглэлтийг дэмжих

- Хурдтай, хүчтэй, уян хатан, дижитал эдийн засгийг хөгжүүлэх;
- АНУ-ын иргэдийн авьяас чадвар, шинэлэг санааг дэмжин хөгжүүлэх, хамгаалах;
- Цахим аюулгүй байдлыг хамгаалах шилдэг ажиллах хүчнийг бий болгох.

[429] https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime/
[430] https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Гуравдугаар хэсэг: Өөрсдийн хүч чадлаар амар амгалан байдлаа хадгалах

- Хариуцлагатай төрийн ажил хэргээр дамжуулан цахим орчны тогтвортой байдлыг бэхжүүлэх;
- Цахим орчин дахь хүлээн зөвшөөрөгдөхгүй үйлдлийг илрүүлэх, таслан зогсоох.

Дөрөвдүгээр хэсэг: АНУ-ын нөлөөг нэмэгдүүлэх

- Нээлттэй, харилцан ашиглах боломжтой, найдвартай, аюулгүй интернэтийг дэмжих;
- Олон улсын кибер чадавхыг бий болгох зэрэг ажлуудыг төлөвлөн, хэрэгжүүлж эхлээд байна.

- 2021 оны Гуравдугаар сард Ерөнхийлөгч Жое Байден **“Богино хугацааны Үндэсний Аюулгүй байдлын Стратегийн Удирдамж”** (Interim National Security Strategic Guidance)-ийг батлан гаргасан байна.[431] Америк улс нь дэлхийн тэргүүлэх гүрний хувьд өөрийн улс үндэстний аюулгүй байдлыг сахин хамгаалахын зэрэгцээ дэлхий дахины аюулгүй байдлыг сахин хамгаалахад баримтлах бодлогыг тус удирдамжид тодорхойлсон байна. Үүнээс цахим аюулгүй байдлаа хамгаалахад шаардагдах дараах ажлуудыг үндэсний хэмжээнд хийхээр төлөвлөсөн байна: Үүнд,

  Шинжлэх ухаан, технологийн баазаа бэхжүүлснээр цахим аюулгүй байдлыг нэн тэргүүний зорилт болгож, цахим орон зайд өөрсдийн чадвар, бэлэн байдал, уян хатан байдлаа бэхжүүлнэ. Цахим аюулгүй байдлыг засгийн газрын бүхий л түвшинд чухлаар авч үзнэ. Нийт Америкчуудад аюулгүй, найдвартай онлайн орчныг бүрдүүлэх, эрсдэлийг даван гарах, хуваалцах үүднээс хувийн хэвшил, засгийн газрын бүх түвшний хамтын ажиллагааг дэмжин ажиллана. Улс орноо кибер халдлагаас үр дүнтэй хамгаалахын тулд дэд бүтцэд оруулсан хөрөнгө оруулалтаа өргөжүүлнэ. Гарал үүсэл харгалзахгүй бүх Америкчуудад боломж олгож, цахим ертөнц дэх авьяаслаг хүний нөөцийг бүрдүүлэх зэрэг ажлуудыг хийхээр төлөвлөсөн байна.
- 2021 оны Тавдугаар сард Ерөнхийлөгч Жое Байден дээрх удирдамж дээр үндэслэн **“Үндэсний Цахим Аюулгүй байдлыг сайжруулах тухай”** (Executive Order on Improving the Nation’s Cybersecurity) зарлигийг батлан гаргасан байна.[432] Тус зарлиг нь дээрх бодлогын баримт бичгүүд дээр үндэслэсэн бөгөөд цахим гэмт хэргийн өнөөгийн нөхцөл байдалд үндэслэн яаралтай хэрэгжүүлэх үйл ажиллагааг 10 багц ажлын хүрээнд төлөвлөсөн байна. Төрийн болон хувийн байгууллагууд руу чиглэсэн цахим халдлагууд, түүнээс сэргийлэх, хамгаалахад шаардагдах нөөц бололцоо, хүчин чармайлтыг нэмэгдүүлэх шаардлагатай байгааг онцолжээ. Үндэсний Стандарт Технологийн Хүрээлэн (National Institute of Standards and Technology) болон Кибер аюулгүй байдлын хамрах хүрээний таван чиг үүргийг тодотгон, Холбооны Засгийн газрын харьяа агентлагууд кибер гэмт хэрэгтнүүд, кибер хорлон сүйтгэх ажиллагаанаас урьдчилан сэргийлэх, илрүүлэх, хариу арга хэмжээ авах зэрэгт хүчин

[431] https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf
[432] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

чармайлтаа нэмэгдүүлэн, нэгдэн ажиллах шаардлагатай байгааг илэрхийлсэн байна. Зарлигт тодотгосноор, Холбооны бүх мэдээллийн систем нь кибер аюулгүй байдлын тодорхой шаардлагуудыг хангасан байх шаардлагатай гэжээ.

III. Цахим гэмт хэрэгтэй тэмцэх байгууллагууд

Цахим гэмт хэрэг нь дан ганц байгууллагын хариуцан хэрэгжүүлэх ажил биш бөгөөд Холбооны Засгийн газрын харьяа агентлагууд, хувийн байгууллагууд болон ашгийн бус олон нийтийн байгууллагууд, түүнчлэн олон улсын байгууллагуудын хамтын хүчин чармайлт шаарддаг байна.

Холбооны Засгийн газрын харьяа агентлагууд

- Батлан Хамгаалах Яам (Department of Defense)-ны харьяа Үндэсний Аюулгүй байдлын Агентлаг (National Security Agency) нь АНУ-ын харилцаа холбооны сүлжээ, мэдээллийн системийг хамгаалах, гадны улс орнуудаас ирэх цахим халдлагыг таслан зогсоох, урьдчилан сэргийлэх үйл ажиллагааг хэрэгжүүлэн ажилладаг.
- Дотоодыг Аюулаас хамгаалах Яам (Department of Homeland Security)-ны харьяа Цахим Аюулгүй байдал, Дэд бүтцийн Аюулгүй байдлын Агентлаг (Cybersecurity and Infrastructure Security Agency) нь 2018 онд байгуулагдсан бөгөөд засгийн газрын бүх түвшинд цахим аюулгүй байдлыг ханган, улс орон даяар цахим аюулгүй байдлын хөтөлбөрийг хэрэгжүүлж, холбооны цахим сүлжээ, цахилгаан станц, далан гэх мэт улс орны чухал дэд бүтцүүдийн аюулгүй, тогтвортой байдлыг ханган ажилладаг.
- Дотоодыг Аюулаас хамгаалах Яамны харьяа АНУ-ын Тагнуулын газар (US Secret Service) нь дотоодын болон олон улсын кибер гэмт хэрэгтнүүдийг илрүүлэх чиг үүрэг бүхий Цахим гэмт хэрэгтэй тэмцэх хэлтэстэй байна. Кибер тагнуулын хэлтэс нь үндэстэн дамнасан кибер гэмт хэрэгтнүүдийг баривчлахад онцгой үүрэгтэй ажилладаг байна. Үүний сацуу Тагнуулын газар нь хууль сахиулах ажилтнууд, прокурор, шүүгч нарт кибер гэмт хэрэгтэй тэмцэх зорилгоор кибер сургалт явуулж, мэдээлэл өгдөг байна.
- Хууль зүйн яам (Department of Justice)-ны харьяа агентлаг Холбооны Мөрдөх Товчоо (Federal Bureau of Investigation) нь чиг үүргээрээ мөн цахим гэмт хэрэгтэй тэмцдэг. Цахим гэмт хэргээс урьдчилан сэргийлэх, тэмцэх ажлын хүрээнд шинээр бүтээгдсэн орчин үеийн дэвшилтэт техник болон аналитик хэрэгслүүдийг үйл ажиллагаандаа ашигладаг байна.
    - Холбооны Мөрдөх Товчоо нь өөрийн 56 салбартаа тусгайлан бэлтгэсэн цахим гэмт хэрэгтэй тэмцэх тасгийг ажиллуулдаг байна. Тухайн тасаг нь үүргээ гүйцэтгэхдээ бусад агентлагийн алба, тасгуудтай хамтран ажиллана.
    - Томоохон гэмт хэргийг илрүүлэн, яаралтай хариу арга хэмжээ авах шаардлагатай тохиолдолд хэдхэн цагийн дотор улс орон даяар Кибер ажиллагааны шуурхай багийг бүрдүүлэн ажиллуулна.
    - Дэлхийн улс орнууд дахь АНУ-ын Элчин сайдын яамдад тухайн улсын болон олон улсын байгууллагуудтай хамтран ажиллах кибер гэмт хэрэгтэй тэмцэх төлөөлөгчийг томилон ажиллуулдаг.
    - Интернэт гэмт хэргийн талаар гомдол хүлээн авах төв (Internet Crime Complaint Center) нь олон нийтээс интернэт гэмт хэргийн талаарх гомдлыг

хүлээн авдаг. Гомдлыг хүлээн авснаар тус төвийн Иргэдийн хөрөнгийг буцаан авах, эргэн төлүүлэх баг нь кибер гэмт хэргийн хохирогчдод хэдэн зуун мянган долларыг эргүүлэн авахад тусалдаг байна.

- 7 хоногийн 24 цагаар тасралтгүй ажилладаг Кибер Хяналт (CyWatch)-ын төв нь улс орон даяар үйл ажиллагаа явуулж буй бусад салбаруудтай холбогдон, гарсан гэмт хэргийн талаар мэдээлэл өгөн, хяналт тавьж ажилладаг.
- Холбооны Мөрдөх Товчоо нь кибер гэмт хэрэгтэй тэмцэх үйл ажиллагаанд АНУ-ын Засгийн газрын туршлагатай мэргэжилтэн, шинжээчдээс бүрдсэн Үндэсний Батлан хамгаалах цахим холбоо (National Defence Cyber Alliance) болон хууль хэрэгжүүлэгчид, хувийн хэвшлийн төлөөллүүд, эрдэм шинжилгээний байгууллагуудаас бүрдсэн Үндэсний Кибер гэмт хэргийг илрүүлэх Сургалтын Холбоо (National Cyber Forensics and Training Alliance)-той хамтран ажилладаг байна.
- АНУ-ын засгийн газрын бусад агентлагууд болох тагнуул болон хууль хэрэгжүүлэгч 30 орчим агентлагаас бүрдсэн Үндэсний Кибер эрэн сурвалжлах хамтарсан баг (National Cyber Investigative Joint Task Force) 2008 онд байгуулагдан, үйл ажиллагаа явуулж буй бөгөөд Холбооны Мөрдөх товчоо тэргүүлдэг байна.

- Хууль зүйн яамны Хүүхдийг садар самуун, бэлгийн мөлжлөгөөс хамгаалах алба (Child Exploitation and Obscenity Section) нь 1987 онд байгуулагдсан бөгөөд садар самууныг сурталчлахаас урьдчилан сэргийлэх, энэ төрлийн гэмт хэргээс хүүхдийг хамгаалах үндсэн чиг үүрэгтэй бөгөөд 2002 онд Дэвшилтэт технологи ашиглан мөрдөн шалгах нэгж (High Technology Investigative Unit)-ийг дотооддоо байгуулан, орон даяар үйл ажиллагаа явуулдаг 94 салбар нэгжээр дамжуулан, цахимаар үйлдэгдэх энэ төрлийн гэмт хэргээс урьдчилан сэргийлж, илрүүлж ажиллах болсон байна. Тус алба нь 2006 оноос Аюулгүй хүүхэд нас хөтөлбөрийг хэрэгжүүлж эхэлжээ.[433]
- Үндэсний Стандарт Технологийн Хүрээлэн нь кибер аюулгүй байдлыг хамгаалахад баримтлах стандартыг боловсруулан, мөрдүүлж ажилладаг байна.

IV. Хууль эрх зүйн орчин

Тус улсад цахим гэмт хэргийг зохицуулсан бие даасан хууль байхгүй бөгөөд холбооны хууль болон мужийн хуулиудаар зохицуулж байна. Компьютерт хууль бусаар нэвтрэхийг хориглох тухай хууль (Computer Fraud and Abuse Act), Холбооны Мэдээллийн Аюулгүй байдлын Менежментийн тухай хууль (Federal Information Security Management Act), Цахим Харилцаа холбооны Нууцлалын тухай хууль (Electronic Communications Privacy Act), Цахим Аюулгүй байдлын мэдээлэл солилцох тухай хууль (Cybersecurity Information Sharing Act) болон холбогдох бусад хууль тогтоомжоор цахим орчин дахь харилцааг зохицуулж байна.

Компьютерт хууль бусаар нэвтрэхийг хориглох тухай хууль[434]

Энэ хуулиар холбооны засгийн газар, банк болон интернэтэд холбогдсон бүх компьютерт

[433] https://www.justice.gov/criminal-ceos
[434] https://www.congress.gov/bill/99th-congress/house-bill/4718

хууль бусаар, зөвшөөрөлгүй нэвтрэх, халдах (hacking)-тай холбоотой асуудлыг зохицуулна. Компьютерт хууль бусаар нэвтрэн аюул учруулах, хохироох, тагнан турших зэрэг гэмт хэргүүд, түүнд ногдох ял шийтгэлийг энэ хуулиар зохицуулсан байна.

Холбооны Мэдээллийн Аюулгүй байдлын Менежментийн тухай хууль[435]

Энэ хуулиар Холбооны Засгийн газрын харьяа агентлаг бүр өөрийн дотоод үйл ажиллагаагаа хэрхэн явуулах болон хамтран ажилладаг байгууллагуудтайгаа хэрхэн харьцах, мэдээлэл түүчлэн агентлагийн хөрөнгийг хэрхэн гадны халдлагаас хамгаалах зэрэг цахим аюулгүй байдлын стандартыг боловсруулан, мөрдөж ажиллахыг шаарддаг байна.

Цахим Харилцаа холбооны Нууцлалын тухай хууль[436]

Тус хуулиар цахимаар мэдээ мэдээлэл дамжуулах, компьютерт хадгалагдсан мэдээлэл болон интернэт хэрэглэгчдийн хувийн нууцыг хэрхэн хамгаалах зэрэг үйлчилгээ үзүүлэгч байгууллага болон хэрэглэгчийн хооронд үүсэх харилцаа, хүлээх үүрэг хариуцлагыг зохицуулсан байна.

Цахим Аюулгүй байдлын мэдээлэл солилцох тухай хууль[437]

Тус хуулиар улсын болон хувийн байгууллага, компаниуд АНУ дахь цахим аюулгүй байдлыг сайжруулах, өөрийн үйл ажиллагааг цахим халдлагаас хамгаалах, урьдчилан сэргийлэх үүднээс цахим аюул, халдлагын талаарх мэдээллийг засгийн газарт мэдээлэх, хуваалцах, харилцан хүлээх үүрэг хариуцлагын талаар хуульчилсан байна.

АНУ-д цахим гэмт хэргийн төрөл болох цахим хүчирхийлэл (cyber violence), ихэвчлэн энэ төрлийн гэмт хэргийн золиос болдог хүүхэд хамгааллын асуудал анхаарлын төвд байсаар байна. Цахим хүчирхийлэл, түүний хэлбэр болох хүүхдэд хор хөнөөлтэй материал үзүүлэх, хүүхдийг садар самуунд уруу татах, хулгайлах, бэлгийн мөлжлөгийн золиос болгох зэрэг гэмт хэргүүдээс хүүхэд, өсвөр үеийнхнийг хамгаалах, урьдчилан сэргийлэх нэлээдгүй хууль тогтоомжийг баталсан байна. Үүнд, Цахим ертөнцөд хүүхдийн нууцыг хамгаалах тухай хууль (Children’s Online Privacy Protection Act), Интернэт орчинд хүүхдийг хамгаалах тухай хууль (Children’s Internet Protection Act), Хүүхэд хамгаалал, аюулгүй байдлын тухай хууль (Child Protection and Safety Act), 21-р зуунд хүүхдийг хамгаалах тухай хууль (Protecting Children in the 21st Century Act), Домэйн нэр үнэн зөв байх тухай хууль (Truth in Domain Names Act), Цахим гэмт хэргийн мэдээллийн шинэчлэлийн тухай хууль (Cybertipline Modernization Act) болон холбогдох бусад хууль тогтоомжоор цахим ертөнц дэх хүүхдийн эрхийг хамгаалдаг байна.

Цахим ертөнцөд хүүхдийн нууцыг хамгаалах тухай хууль[438]

Тус хуулиар 13-аас доош насны хүүхэд цахим хуудсанд хандаж байгаа тохиолдолд эцэг, эхийнх нь зөвшөөрөлгүйгээр хувийн мэдээллийг нь авахгүй байх талаар хуульчилсан байна. Хэрэглэгчдийн эрх ашгийг хамгаалах үүрэг бүхий Холбооны Худалдааны Комисс нь тус хуулийг хэрэгжүүлэх журмыг баталсан бөгөөд 2012 онд шинэчлэн баталж, хууль зөрчсөн компаниудад зохих арга хэмжээг ногдуулсаар ирсэн байна.

[435] https://www.congress.gov/bill/107th-congress/house-bill/3844
[436] https://www.sciencedirect.com/topics/computer-science/electronic-communications-privacy-act
[437] https://www.congress.gov/bill/114th-congress/senate-bill/754/text
[438] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security/kids-privacy-coppa https://www.law.cornell.edu/uscode/text/15/chapter-91

Интернэт орчинд хүүхдийг хамгаалах тухай хууль[439]

Тус хуулиар хүүхдийг интернэтээр зохисгүй, садар самуун материал харах, үзэхээс сэргийлсэн зохицуулалтыг хийсэн байна. Сургууль, номын сангууд нь компьютертэ зохисгүй материалыг шүүх програмыг суулгах шаардлагатай бөгөөд интернэтийн аюулгүй байдлын бодлогыг баримтлан хэрэгжүүлдгээ баталгаажуулаагүй тохиолдолд E-rate хөтөлбөрөөс олгодог интернэтийн хөнгөлөлтийг эдлэх боломжгүй болох юм. Холбооны Харилцаа холбооны хороо нь (Federal Communication Commission) тус хуулийг хэрэгжүүлэх журмыг 2001 оны эхээр батлан, 2011 онд шинэчлэн баталсан байна.

Хүүхэд хамгаалал, аюулгүй байдлын тухай хууль[440]

Энэ хуулийг хүчирхийллийн золиос болсон Адам Валш хүүгийн нэрээр нэрлэсэн байна. Энэ хуулиар цахим хуудас хайх явцад санаатайгаар хүнийг төөрөгдүүлсэн нэр хаяг, зураг тавьж хүмүүс, насанд хүрээгүй хүүхдийг садар самуунд уруу татах, хүүхдэд зохисгүй, хортой контент үзүүлэхийг хориглосон байна.

Түүнчлэн энэ хуулиар улс орон даяар хүчингийн хэрэгт холбогдож байсан гэмт этгээдүүдийг бүртгэлжүүлэхийг үүрэг болгосон байна. Гэмт этгээдүүдийг гэмт хэргийн шинжээс хамааран 3 ангилалд (Tier 1, 2, 3) ангилах бөгөөд 2-хүнд, 3-онц хүнд хэрэг үйлдсэн этгээдүүдийн талаарх мэдээллийг олон нийтэд нээлттэй байршуулахыг муж, орон нутгийн хууль сахиулагчдад үүрэг болгосон байна.

- 1-р ангиллын гэмт хэрэгтнүүд 15 жилийн турш, жил бүр оршин суугаа газрынхаа цагдаагийн газарт бүртгүүлнэ.
- 2-р ангиллын гэмт хэрэгтнүүд 25 жилийн турш, 6 сар тутам оршин суугаа газрынхаа цагдаагийн газарт бүртгүүлнэ.
- 3-р ангиллын гэмт хэрэгтнүүд насан туршдаа, 3 сар тутам оршин суугаа газрынхаа цагдаагийн газарт бүртгүүлнэ.

Бүртгэл хийлгээгүй тохиолдолд хууль зөрчсөнд тооцон, хариуцлага хүлээлгэнэ.

21-р зуунд хүүхдийг хамгаалах тухай хууль[441]

Энэ хуулиар хэрэглэгчдийн эрх ашгийг хамгаалах үүрэг бүхий Холбооны Худалдааны Комисст Хүүхдийн аюулгүй интернэт хэрэглээг дэмжих хөтөлбөр боловсруулан улс орон даяар хэрэгжүүлэхийг үүрэг болгосон байна. Тус хөтөлбөр нь төрийн болон хувийн хэвшлийн байгууллагуудын хэрэглэж буй интернэтийн аюулгүй байдлыг хангах арга хэрэгслүүдээс шилдэг туршлагыг шалгаруулан, урамшуулах, олон нийтэд түгээх, танилцуулах, ялангуяа интернэтийн аюулгүй болон зохистой хэрэглээ, цахим орчинд олон нийтийн сүлжээгээр үл таних хүнтэй хэрхэн харилцах, цахимаар доромжлох, дээрэлхэх үйлдлээс хэрхэн сэргийлэх, хариу өгөх талаар хүүхэд, өсвөр насныханд сургах, таниулах сургалтын хөтөлбөрүүдийг багтаасан байх шаардлагатай байна. Холбооны Худалдааны Комисс нь жил бүр Конгресст хуулиар хүлээсэн энэхүү үүргийнхээ хэрэгжилтийн тайланг танилцуулах шаардлагатай байна.

[439] https://www.fcc.gov/consumers/guides/childrens-internet-protection-act
[440] https://www.congress.gov/bill/108th-congress/senate-bill/800/text
[441] https://www.ftc.gov/enforcement/statutes/protecting-children-21st-century-act
https://www.law.cornell.edu/uscode/text/15/chapter-91A

Домэйн нэр үнэн зөв байх тухай хууль[442]

Тус хуулиар хүмүүст болон насанд хүрээгүй хүүхдэд интернэтээр зохисгүй материал үзүүлэх, садар самуунд уруу татах зорилгоор хуурамч домэйн нэр ашиглахыг хориглосон байна. Хэрэв санаатайгаар хуурамч домэйн нэр ашиглан, хүнийг төөрөгдүүлэн садар самуунд уруу татсан тохиолдолд мөнгөн торгууль ногдуулах буюу 2 жилээс ихгүй хугацаагаар хорих эсхүл мөнгөн торгууль ногдуулах болон хорих шийтгэл давхар ногдуулна. Хэрэв санаатайгаар хуурамч домэйн нэр ашиглан, хүүхдийг төөрөгдүүлэн садар самуунд уруу татсан тохиолдолд мөнгөн торгууль ногдуулах буюу 10 жилээс ихгүй хугацаагаар хорих эсхүл мөнгөн торгууль ногдуулах болон хорих шийтгэл давхар ногдуулна гэж заажээ.

Цахим гэмт хэргийн мэдээллийн шинэчлэлийн тухай хууль[443]

АНУ-д үйл ажиллагаа явуулж байгаа цахимаар үйлчилгээ эрхлэгчид нь хүүхдийг бэлгийн хүчирхийлэл, садар самуун үйлдэлд ашигласан материалын талаар мэдсэн тохиолдолд хууль сахиулагч байгууллагад нэн даруй мэдэгдэх үүрэгтэй байна.

Арьс өнгө, гарал үүсэл, нас хүйс, шашин шүтлэг, хөгжлийн бэрхшээл зэргээр нь ялгаварлан гадуурхаж, айлган сүрдүүлсэн (Cyber bullying, Cyber harassment) тохиолдолд **Ялгаварлан гадуурхах гэмт хэргээс урьдчилан сэргийлэх тухай (Hate Crimes Prevention Act)**[444] хуулиар зохицуулдаг байна.

Нэгдсэн Улсын Код, Сэдэв 18 - Гэмт хэрэг болон Гэмт хэргийн үйл явц, Бүлэг 110A, Хэсэг 2261A-аар Мөшгих болон Цахимаар мөшгих (Cyber stalking) гэмт хэргийг зохицуулсан байна.[445]

4.2 БҮГД НАЙРАМДАХ СОЛОНГОС УЛС

I. Цахим орчин дахь гэмт хэргийн нөхцөл байдал:

2020 оны байдлаар БНСУ-ын цагдаагийн байгууллагад 234 мянга орчим цахим гэмт хэрэг бүртгэгдсэн ба энэ нь өмнөх оноос 54 мянга орчим хэргээр нэмэгдсэн байна. Цахим гэмт хэргийн хамгийн түгээмэл тохиолдлуудад интернэтийн залилан, санхүүгийн залилан, гэх мэт мэдээллийн сүлжээний гэмт хэрэгүүд бүртгэгдсэн байна.[446]

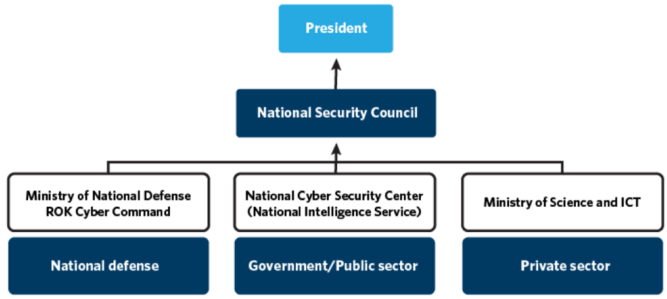
II. Цахим аюулгүй байдлын засаглал

Сүүлийн жилүүдэд Засгийн газар цахим халдлагын талаар ихээхэн анхаарал хандуулж бодлогын түвшинд авч үзсэн байна. Цахим засаглалын хувьд 3 агентаас бүрддэг.[447] Үүнд:

1. Үндэсний тагнуулын албаны дэргэдэх Цахим аюулгүй байдлын үндэсний төв (National Cybersecurity Center)
2. Шинжлэх ухаан мэдээлэл технологийн яам (Ministry of Science and ICT)
3. Үндэсний Батлан хамгаалах яам (Ministry of National Defense)

[442] https://www.law.cornell.edu/uscode/text/34/subtitle-II/chapter-209
[443] https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2258A&num=0&edition=prelim
[444] https://www.fbi.gov/investigate/civil-rights/federal-civil-rights-statutes
[445] https://www.law.cornell.edu/uscode/text/18/2261A#
[446] https://www.statista.com/statistics/1222208/south-korea-cyber-crime.
[447] https://carnegieendowment.org/2021/08/17/korean-policies-of-cybersecurity-and-data-resilience-pub-85164

Зураг 1. Цахим аюулгүй байдлын засаглалын схем[448]



Source: NIS et. al., “White Paper on Information Security 2018” (in Korean), 2018, p. 52.

БНСУ-д 2015 оноос эхлэн Ерөнхийлөгчид шууд харьяалагддаг Үндэсний аюулгүй байдлын зөвлөл (ҮАБЗ) нь кибер аюулгүй байдалтай холбоотой асуудлуудыг зохицуулж ирсэн байна.[449] Үндэсний аюулгүй байдлын зөвлөлийн доорх Цахим аюулгүй байдлын үндэсний төв нь цахим гэмт хэрэг, халдлага аюулгүй байдалтай холбоотой асуудлуудыг хариуцан ажилладаг байна. Цахим аюулгүй байдлын үндэсний төв нь Шинжлэх ухаан мэдээлэл технологийн яам болон Үндэсний Батлан хамгаалах яамтай хамтран хувийн хэвшил болон төрийн байгууллагуудын цахим аюулгүй байдлыг хариуцаж хоорондоо уялдаатай ажилладаг байна.

III. Цахим орчин дахь гэмт хэргийн стратеги төлөвлөгөө

Өмнөд Солонгос Улс төрөл бүрийн кибер халдлага гэмт хэргээс сэргийлэн 2019 онд Кибер аюулгүй байдлын үндэсний стратегийг боловсруулжээ. Уг стратеги нь 6 зорилттой байна. Үүнд:

1. Үндэсний дэд бүтцийн аюулгүй байдлыг нэмэгдүүлэх (Increase the Safety of National Core Infrastructure)

- Үндэсний мэдээлэл, харилцаа холбооны сүлжээний аюулгүй байдлыг бэхжүүлэх;
- Кибер аюулгүй байдлын орчны дэд бүтцийг сайжруулах;
- Шинэ үеийн кибер аюулгүй байдлын дэд бүтцийг хөгжүүлэх.

2. Кибер халдлагын хариу арга хэмжээ түүний хүчин чадлыг сайжруулах (Enhance Cyber Attack Response Capabilities)

- Кибер халдлагаас урьдчилан сэргийлэх;
- Том хэмжээний кибер халдлагын эсрэг бэлэн байдлыг бэхжүүлэх;
- Кибер халдлагын эсрэг цогц, идэвхтэй арга хэмжээ авах;
- Цахим гэмт хэрэгтэй тэмцэх чадварыг сайжруулах.

[448] NIS et al., “White Paper on Information Security 2004” (in Korean), 2004, p. 7.
[449] From 2015 to 2018, the NSC designated the cybersecurity adviser to lead the cybersecurity efforts nation-wide, however, this position was merged with the cyber information convergence adviser under the same NSC

3. Итгэлцэл, хамтын ажиллагаанд суурилсан засаглалыг бий болгох (Establish Governance Based on Trust and Cooperation)

- Төр, хувийн хэвшил, цэргийн хамтын ажиллагааны тогтолцоог сайжруулах;
- Улс даяар мэдээлэл солилцох системийг бий болгох;
- Кибер аюулгүй байдлын эрх зүйн үндсийг сайжруулах.

4. Кибер аюулгүй байдлын салбарын өсөлтийг дэмжих (Build Foundations for Cybersecurity Industry Growth)

- Кибер аюулгүй байдлын хөрөнгө оруулалтыг нэмэгдүүлэх;
- Кибер аюулгүй байдлын ажиллах хүч, технологийн өрсөлдөх чадварыг бэхжүүлэх;
- Кибер аюулгүй байдлын компаниудыг хөгжих орчныг бүрдүүлэх;
- Кибер аюулгүй байдлын зах зээлд шударга өрсөлдөөний зарчмыг бий болгох.

5. Кибер аюулгүй байдлын соёлыг бий болгох (Foster a Cybersecurity Culture)

- Кибер аюулгүй байдлын талаар мэдлэгийг дээшлүүлэх, кибер аюулгүй байдлын практикийг бэхжүүлэх;
- Үндсэн эрхийг кибер аюулгүй байдалтай тэнцвэржүүлэх.

6.Кибер аюулгүй байдлын чиглэлээр олон улсын хамтын ажиллагааг нэмэгдүүлэх (Lead International Cooperation in Cybersecurity)

- Хоёр талын болон олон талт хамтын ажиллагааны системийг сайжруулах;
- олон улсын хамтын ажиллагааг манлайлах.

IV. Хууль эрх зүйн орчин

БНСУ-ын Эрүүгийн хуульд цахим гэмт хэрэгтэй холбоотой дараах зохицуулалтууд байдаг. Үүнд:[450] Эрүүгийн хууль (Criminal Law)

- Зүйл 141. Олон нийтийн баримт бичиг, нийтийн хэрэгсэлд хохирол учруулах (The invalidity of Public Documents, etc. and Destruction of Public Goods) Төрийн албанд ашигладаг баримт бичиг, бусад хэрэгсэл, дуу бичлэг гэх мэт тусгай хэвлэл мэдээллийн хэрэгслийг гэмтээж, нуун дарагдуулсан, сүйтгэсэн этгээдийг 7 жил хүртэлх хорих ял эсвэл 10 сая хүртэлх воноор торгоно.
- Зүйл 227-2. Нийтийн дуу бичлэгийг хуурамчаар бэлтгэх буюу өөрчлөх (False Preparation or Alteration of Public Electromagnetic Records)
  Хэрэв үүнтэй холбоотой зөрчил үүсгэвэл 10 хүртэлх жилээр хорих шийтгэлтэй байна.
- Зүйл 316. Нууц задруулах (Violation of Secrecy) Битүүмжилсэн эсвэл нууцлалтай захидал, баримт бичиг, зургийг нээсэн этгээдийг 3 жил хүртэл хорих, эсхүл таван сая воноор торгууль ногдуулна.
- Зүйл 347-2. Компьютер ашиглах замаар залилан хийх (Fraud by The Use of Computer, etc.) Хэн нэгэн хөндлөнгийн этгээд компьютер ашиглан бусдын зөвшөөрөлгүй худал, зохисгүй мэдээлэл ашиглан ашиг хүртэх, хууль зөрчсөн тохиолдолд 10 хүртэлх жилээр хорих эсвэл 20 сая воноор торгоно.

[450] https://www.cybercrimelaw.net/Korea.html

- Зүйл 366. Эд хөрөнгөд халдах, сүйтгэх (Destruction and Damage, etc. of Property) Бусдын эд хөрөнгөтэй холбоотой баримт бичиг, дуу бичлэг гэх мэт мэдээллийн хэрэгслийг устгах, гэмтээх, нуун дарагдуулах, тохиолдолд 3 жил хүртэлх хорих, эсвэл 7 сая хүртэлх воноор торгоно.

БНСУ 1980 оноос эхлэн Үндэсний мэдээллийн аюулгүй байдал болон нийгмийн сүлжээн дэх асуудлуудыг зохицуулах хуулийг боловсруулж эхэлсэн ба 1986 онд Харилцаа холбооны сүлжээг сайжруулах тухай хууль (Expansion and promotion of utilization of communications network act) анх баталж байжээ.[451] Одоогоор кибер аюулгүй байдалтай холбоотой асуудлыг хэд хэдэн хуулиар зохицуулж байна. Тухайлбал:[452]

- Сүлжээний тухай хууль (Network act)
- Харилцаа холбооны нууцыг хамгаалах тухай хууль (Protection of communication secret act)
- Мэдээлэл, харилцаа холбооны дэд бүтцийг хамгаалах тухай хууль (The act on protection of information and communication infrastructure)
- Цахим засаглалын тухай хууль (Electronic government act)
- Үндэсний батлан хамгаалахын мэдээллийн дэд бүтцийг бий болгох, мэдээллийн нөөцийг удирдах тухай хууль (Act on Establishment of infrastructure for information of national defence and management of information resources for national defence)
- Зээлийн мэдээллийн ашиглалт, хамгаалалтын тухай хууль (Credit information use and protection act)
- Байршлын мэдээллийг хамгаалах тухай хууль (Act on protection use of location information)
- Үйлдвэрлэлийн технологийг хамгаалах тухай хууль (Act on Prevention of Divulgence and protection of industrial technology)
- Цахилгаан холбооны бизнесийн болон санхүүгийн луйврын тухай хууль (Telecommunication business act and special act on financial fraud) зэрэг байна.

Үндэсний хэмжээнд кибер халдлагаас сэргийлэх зорилгоор “Кибер аюулгүй байдлын менежментийн зохицуулалтын (National cyber security management regulation) журам”-ыг Үндэсний Ассамблей баталсан байна. Уг журмаар Засгийн газрын байгууллагуудын (Үндэсний тагнуулын албаны Үндэсний аюулгүй байдлын төв, Хөх ордон дахь үндэсний аюулгүй байдлын алба) эрх үүрэг, оролцоог тодорхойлсон байна.[453] Кибер халдлагаас хамгаалах мэдээллийн дэд бүтцийн тухай хууль нь үндэсний аюулгүй байдалтай шууд холбогддог ба эрчим хүч, эрүүл мэнд, банк санхүүгийн цахим үйл ажиллагааг уг хуулиар зохицуулдаг байна. Солонгосын Засгийн газар 2002 онд Мэдээллийн дэд бүтцийг хамгаалах тухай хуулийг (Protecting critical information infrastrucutre act) баталсан байна. Уг хууль нь дараах бүтэцтэй байна.

[451] Introduction to Korean cyber security Law
[452] https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/korea
[453] Ibid Page 28

МЭДЭЭЛЭЛ, ХАРИЛЦАА ХОЛБООНЫ ДЭД БҮТЦИЙГ ХАМГААЛАХ ТУХАЙ ХУУЛЬ

(The Act On Protection Of Information And Communication Infrastructure)

1 дүгээр зүйл. Зорилго

Энэхүү хуулийн зорилго нь харилцаа холбооны нууц, нууцыг хамгаалах, харилцаа холбооны эрх чөлөөг тогтоох, зохих журмын дагуу шийдвэр гаргах замаар харилцаа холбооны эрх чөлөөг зохицуулахад оршино.

2 дугаар зүйл. Нэр томьёоны тайлбар

3 дугаар зүйл. Харилцаа холбооны нууцыг хамгаалах

4 дүгээр зүйл. Хууль бус хяналт шалгалтаар олж авсан мэдээлэл хууль бусаар чагнах, цахилгаан холбооны агуулгыг нотлох баримт болгон ашиглахыг хориглох тухай

5 дугаар зүйл. Эрүүгийн байцаалтын мэдээллийг хязгаарлах зөвшөөрлийн шаадлага

6 дугаар зүйл. Эрүүгийн байцаалтын мэдээллийг хязгаарлах зөвшөөрлийн арга хэмжээ авах эрх олгох журам

7 дугаар зүйл. Үндэсний аюулгүй байдалд нийцүүлсэн харилцаа холбооны хяналт

8 дугаар зүйл. Онцгой байдлын үеийн харилцаа холбоог хязгаарлах арга хэмжээ

9 дүгээр зүйл. Харилцаа холбоонд хяналт тавих арга хэмжээний хэрэгжилт

10 дугаар зүйл. Чагнах төхөөрөмжийн зөвшөөрөл олгох журам

11 дүгээр зүйл. Нууцлалын үүрэг

12 дугаар зүйл. Харилцаа холбооны арга хэмжээгээр олж авсан материалыг ашиглахыг хязгаарлах тухай

13 дугаар зүйл. Эрүүгийн байцаан шийтгэх үйл ажиллагаанд мэдээлэл өгөх журам

14 дүгээр зүйл. Бусдын нууцыг задруулсан зөрчлийн тухай

15 дугаар зүйл. Үндэсний Ассамблейн хяналт

16 дугаар зүйл. Торгуулийн заалт

17 дугаар зүйл. Торгууль оногдуулах тухай

18 дугаар зүйл. Гэмт хэрэг үйлдэхийг завдах тухай

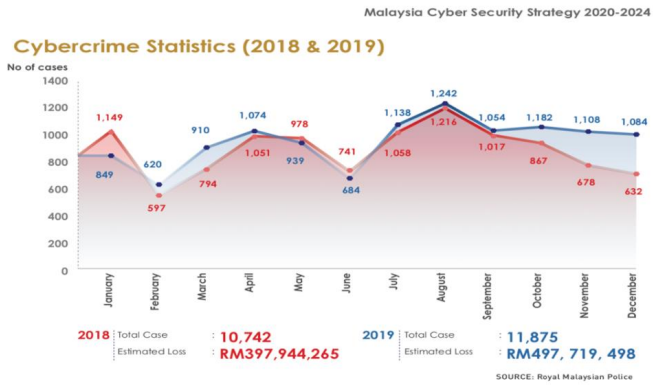
4.3 МАЛАЙЗ УЛС

I. Цахим орчин дахь гэмт хэргийн нөхцөл байдал

Ковид-19 цар тахлын үед цахим технологийн хэрэглээ өсөж байгаа нь кибер гэмт хэргийн гаралтыг нэмэгдүүлж, Малайз Улсын аюулгүй байдалд нөлөөлж байна. Малайзын цагдаагийн байгууллагын мэдээлснээр 2019 онд кибер халдлага, гэмт хэргийн тоо 3,787 байсан бол 2020 он гэхэд эдгээр халдлагууд 4,194 болж, 10%-аар нэмэгдсэн байна. 2021 онд энэ тоо цаашид нэмэгдэх төлөвтэй байна.[454]

[454] Малайз Улс Кибер гэмт хэргийн нөхцөл байдал The Star Hews https://www.thestar.com.my/news/nation/2021/06/28/cybercrime-increasing-as-more-people-rely-on-digital-tech-during-pandemic-says-pm

Зураг 2. Малайз Улсын кибер гэмт хэргийн статистик



II. Цахим орчин дахь гэмт хэргийн стратеги төлөвлөгөө

Малайз Улсын кибер аюулгүй байдлын стратеги нь[455] (Malaysia Cyber Security Strategy) 2020-2024 онд кибер аюулгүй байдлын төлөвлөлт, хэрэгжилтийг бүх талаар зохицуулах 5 чиглэлд хэрэгжихээр боловсруулагдсан байна.

1. Үр дүнтэй засаглал ба удирдлага (Effective Governance and Management)
2. Эрх зүйн хүрээ, гүйцэтгэлийг сайжруулах (Strengthening legislative framework and enforcement)
3. Дэлхийн түвшний инновац, технологи, судалгаа ба аж үйлдвэр (Catalysing World Class Innovation, Technology, R&D and Industry)
4. Чадавхыг дээшлүүлэх, мэдлэг, боловсролыг нэмэгдүүлэх (Enhancing Capacity and Capability Building, Awareness and Education)
5. Олон Улсын хамтын ажиллагааг бэхжүүлэх (Strengthening Global Collaboration)

Дээрх Малайз улсын кибер аюулгүй байдлын стратегит Засгийн газар, бизнес, нийгмийн (иргэд) янз бүрийн салбарт кибер аюулгүй байдлыг сайжруулахад чиглэсэн үйл ажиллагаануудын төлөвлөгөөг тодорхойлсон.

Үр дүнтэй засаглал ба удирдлага (Effective Governance and Management)

Стратеги 1. *Үндэсний кибер аюулгүй байдлын засаглал, экосистемийг сайжруулах;*
Стратеги 2. *Байгууллагын менежмент ба бизнесийн үйл ажиллагааг сайжруулах (Засгийн газар, Үндэсний мэдээллийн дэд бүтэц ба Бизнес);*
Стратеги 3. *Кибер аюулгүй байдлын ослын менежмент, кибер хамгаалалтыг идэвхжүүлэх.*

[455] Malaysia Cyber Security Strategy (2020-2024) https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

Эрх зүйн хүрээ, гүйцэтгэлийг сайжруулах (Strengthening legislative framework and enforcement)

Стратеги 4. *Кибер гэмт хэрэг, халдлагыг хязгаарлах бууруулах кибер аюулгүй байдлын хуулийг сайжруулах;*
Стратеги 5. *Цахим гэмт хэрэгтэй тэмцэх чадавх, чадварыг сайжруулах.*

Дэлхийн түвшний инновац, технологи, судалгаа ба аж үйлдвэр (Catalysing World Class Innovation, Technology, R&D and Industry)

Стратеги 6. *Үндэсний кибер аюулгүй байдлын судалгаа, шинжилгээний хөтөлбөрийг идэвхжүүлэх;*
Стратеги 7. *Өрсөлдөх чадвартай дотоодын үйлдвэрлэл, технологийг дэмжих.*

Чадавхыг дээшлүүлэх, мэдлэг, боловсролыг нэмэгдүүлэх (Enhancing Capacity and Capability Building, Awareness and Education)

Стратеги 8. *Үндэсний кибер аюулгүй байдлын чадавхыг бэхжүүлэх;*
Стратеги 9. *Кибер аюулгүй байдлын талаарх мэдлэгийг дээшлүүлэх;*
Стратеги 10. Боловсролоор дамжуулан кибер аюулгүй байдлын талаар мэдлэгийг нэмэгдүүлэх.

Олон Улсын хамтын ажиллагааг бэхжүүлэх (Strengthening Global Collaboration)

Стратеги 11. *Кибер аюулгүй байдлын асуудлаарх олон улсын хамтын ажиллагааг бэхжүүлэх;*
Стратеги 12. Олон улсын аюулгүй байдлыг сахин хамгаалахын тулд аюулгүй, тогтвортой, энх тайван кибер орон зайг дэмжих тухай амлалтаа зарлах.

IV. Хууль эрх зүйн орчин

Малайз Улс кибер аюулгүй байдалтай холбоотой дараах цогц хуулиудыг баталсан байна. (**Хавсралт 4)** Үүнд:

- Зохиогчийн эрхийн тухай хууль (The Copyright (AmendmentAct)
- Тоон гарын үсгийн тухай хууль (The Digital Signature Act)
- Телемедициний тухай хууль (The Telemedicine Act)
- Харилцаа холбоо ба мультимедиан тухай хууль (The Communications and Multimedia Act)
- Цахим худалдааны тухай хууль(Electronic Commerce Act)
- Төрийн цахим үйл ажиллагааны тухай хууль (Electronic Government Activities Act)
- Хувийн мэдээллийг хамгаалах тухай хууль (Personal Data Protection Act) Эрүүгийн хууль (Penal Code)
- Хуурамч мэдээллийн эсрэг хууль (The Anti-Fake News Act) гэх мэт.

Малайз Улс 1997 онд Компьютерийн гэмт хэрэгтэй тэмцэх тухай хуулийг (The Computer Crimes Act) баталсан ба 2011 оны 12-р сарын 1-нд дахин шинэчилсэн байна. Уг хуулиар зохицуулж буй харилцаа:[456]

[456] https://cyrilla.org/ar/entity/xqej2atn2lh?file=1568729651356shamgdeopv.pdf&page=5

КОМПЬЮТЕРИЙН ГЭМТ ХЭРЭГТЭЙ ТЭМЦЭХ ТУХАЙ ХУУЛЬ, 1997 ("ССА")

Бүлэг 1. **Зорилт**

Нэр томьёоны тайлбар

Бүлэг 2.

Компьютерийн мэдээлэл рүү зөвшөөрөлгүй нэвтрэх

- Бусдын компьютер болон компьютерийн мэдээлэл (дата)-д зөвшөөрөлгүй, санаатайгаар нэвтэрсэн гэм буруутай нь тогтоогдвол 50 мянган ринггитээс ихгүй торгууль ногдуулах буюу таван жилээс дээшгүй хугацаагаар хорих шийтгэл ногдуулна.

Өөрөө болон бусад хүнээр халдлага үйлдэх,

- Энэ хэсэгт заасны дагуу гэмт хэрэг үйлдсэн гэм буруутай этгээдэд 150 мянган ринггитээс ихгүй хэмжээний торгууль ногдуулах, эсхүл арван жилээс дээшгүй хугацаагаар хорих ялаар шийтгэнэ.

Аливаа компьютерийн өгөгдөл агуулгыг зөвшөөрөлгүй өөрчлөх

- Бусдын компьютерийн агуулгыг зөвшөөрөлгүй өөрчлөх үйлдэл хийсэн тохиолдолд 100-500 мянган ринггитээс дээшгүй торгууль ногдуулах, эсхүл долоогоос арван жилийн хорих ялаар шийтгэнэ.

Зөвшөөрөлгүй харилцах

- Компьютерт нэвтрэх дугаар, код, нууц үг эсвэл бусад хэрэгслийг шууд болон дам байдлаар мэдэгдсэн тохиолдолд 25 мянган ринггитээс дээшгүй торгууль ногдуулах, эсхүл гурван жил хорих ялаар шийтгэнэ.

Бүлэг 3.

Нэмэлт болон ерөнхий заалтууд[457]

Халдлагын цар хүрээ

- Энэхүү хуулийн заалтууд нь гэмт этгээдийн иргэншил болон оршин суух харьяаллаас үл хамааран Малайзын нутаг дэвсгэрт хүчин төгөлдөр үйлчлэх бөгөөд хуульд заасан гэмт хэрэг үйлдсэн этгээдийг хуулийн дагуу шийтгэдэг байна.

Эрэн сурвалжлах, хураах, баривчлах бүрэн эрх

- Энэ хуульд заасны дагуу гэмт хэрэг үйлдсэн болохыг нотлох баримтанд үндэслэх эсвэл шүүгчийн шийдвэр гарвал, байцаагчаас дээш цолтой (above the rank of Inspector) албан хаагч гэмт хэргийн газар хүчээр нэвтрэх, шаардлагатай бол саатуулах, тэнд байгаа нотлох баримтыг хайх, хураах эрхтэй байдаг.

Мөрдлөгт саад учруулах

- Уг хуульд заасны дагуу албан хаагчийн эрх, үүргийн дагуу мөрдлөг хийх явцад халдах, саад учруулах, байцаалтыг хойшлуулахыг хориглодог.

Яллах

- Уг хуулийн дагуу яллах ажиллагааг Улсын яллагчийн албан ёсны шийдвэрээс бусад тохиолдолд яллахгүй.

[457] https://www.nacsa.gov.my/legal.php

4.4 ЯПОН УЛС

I. Цахим орчин дахь гэмт хэргийн нөхцөл байдал[458]

2021 оны 3-р сарын байдлаар Үндэсний цагдаагийн газраас явуулсан судалгаагаар 18-аас доош насны 1819 хүүхэд 2020 онд нийгмийн сүлжээтэй холбоотой гэмт хэргийн хохирогч болсон болохыг тогтоожээ. Хохирогчдын бараг 90 хувь нь бага, ахлах сургуулийн сурагчид байсан бөгөөд үүний 35,3 хувийг твиттер ашиглагч эзэлж байна. Хэдийгээр 2019 оны мөн үетэй (2082) харьцуулахад 12,6%-аар буурсан боловч 2013 оноос хойш сүүлийн 5 жилд 4.6 хувиар өссөн үзүүлэлттэй байжээ. Гэмт хэргийн төрлийг ангиллаар нь авч үзвэл, хүүхдийг хамгаалах хууль, журмыг зөрчсөн 738, хүүхдийг садар самуунд уруу татсан 597, хүүхдийн биеэ үнэлэх явдал 311 байгаа бол хүнд гэмт хэргийн хувьд хулгайлах гэмт хэрэг өссөн үзүүлэлттэй гарчээ. Хохирогчдын нэвтрэх хэрэгслийн хувьд ухаалаг гар утас нь нийт интернэт хэрэглэгчдийн 90 орчим хувийг эзэлж байсан бол ашигладаг сүлжээний хувьд Твиттер дээр 642, Инстеграм дээр 221, Химабе дээр 160, Тик ток дээр 76, Коё Томо дээр 63 байсан байна. 2019 онд онлайн банкны луйврын улмаас 2.5 тэрбум гаруй иений хохирол учирсан байна. 2020 онд телевизийн реалити цуврал нэвтрүүлэгт оролцсон эмэгтэй мэргэжлийн бөх Хана Кимура амиа хорлосонтой холбоотойгоор цахим орчинд дээрэлхэх явдал нь улс оронд томоохон асуудал болжээ.

II. Цахим орчин дахь гэмт хэргийн стратеги төлөвлөгөө

Кибер аюулгүй байдлын стратеги (2021)

2021 оны 9 сард Кибер аюулгүй байдлын 3 дахь стратеги төлөвлөгөөг батлан гаргасан байна. Үндсэн зарчимд мэдээллийн чөлөөт урсгалын баталгаа, хуулийн засаглал, нээлттэй байдал, бие даасан байдал, олон талт хамтын ажиллагаатай байна гэж тусгажээ. Ирэх 3 жилд хэрэгжүүлэх стратегийн зорилго, чиглэлээ:

1. Нийгэм эдийн засгийн тогтвортой хөгжлийг нэмэгдүүлэх:

- Дижитал аюулгүй байдлын мэдлэгийг дээшлүүлэх;
- Орон нутаг болон ЖДҮ эрхлэгчдийн дунд “Цахим аюулгүй байдал бүхий DX”-ийг сурталчлах;
- Сүлжээний найдвартай байдлыг хангах.

2. Аюулгүй байдал, дижитал нийгмийг ухамсарлах:

- Нийгэм болон хүмүүсийг хамгаалах кибер аюулгүй байдлын орчныг бүрдүүлэх;
- Нийгэм, эдийн засгийн дэд бүтцийг түшиглэсэн оролцогч талуудын хүчин чармайлтыг дэмжих;
- Кибер халдлагад хариу өгөх бэлэн байдлыг хангах.

3. Японы үндэсний аюулгүй байдлыг хангах:

- Чөлөөт, шударга, аюулгүй цахим орон зайг хангах;
- Кибер аюулгүй байдлын хамгаалалт, урьдчилан сэргийлэх чадварыг бэхжүүлэх;
- Олон улсын хамтын ажиллагааны оролцоог дээшлүүлэх;
- Хүний нөөцийг бүрдүүлэх, хөгжүүлэх зорилгоор баталсан байна.

[458] Cabinet Office https://www8.cao.go.jp/youth/kankyou/index.html

III. Холбогдох байгууллагууд

Цагдаагийн Ерөнхий газар нь Эрүүгийн хууль болон холбогдох хуулийн дагуу цахим гэмт хэргийг мөрдөн шалгаж, таслан зогсоох үүрэгтэй ажилладаг. Мөн Цагдаагийн Ерөнхий газрын “Кибер гэмт хэрэгтэй тэмцэх төв”-өөс муж бүрийн цагдаа нарт кибер гэмт хэргийн талаар мэдээлэл, заавар зөвлөгөө өгч ажилладаг. Засгийн газрын Хэрэг эрхлэх газар нь хүүхэд, залуучуудын хөгжил, дэмжлэгийн талаар төлөвлөлт, иж бүрэн зохицуулалт хийх үүрэг бүхий төрийн байгууллагын хувьд үндсэн цогц бодлогыг боловсруулсан бөгөөд энэхүү бодлогыг үндэслэн холбогдох яам, агентлагууд орон нутгийн засгийн газар болон бусад холбогдох төрийн болон хувийн хэвшлийн байгууллагууд үйл ажиллагаагаа хэрэгжүүлдэг. Үүнээс гадна интернэт орчинд үйл ажиллагаа явуулдаг GREE, CyberAgent, DeNA, Facebook Japan, Mixi, LINE, Twitter Japan зэрэг операторууд нэгдэн “Өсвөр үеийнхний интернэт ашиглалтын орчныг сайжруулах зөвлөл”-ийг олон нийтийн сайтуудаас үүдэлтэй хүүхдийг гэмтээх аливаа үйлдлээс урьдчилан сэргийлэх хүчин чармайлтыг сурталчлах зорилгоор 2017 онд байгуулсан. Зөвлөл нь хүүхдийн аюулгүй интернэт орчныг бүрдүүлэхээр мэдээлэл солилцох, судалгаа, боловсрол, соён гэгээрүүлэх үйл ажиллагаа явуулдаг. Мөн Ignis, Cocone, Nanameue, Moi, Yudo, ITI, C studio, Social Town, Maleo зэрэг компаниуд хамтран оролцох болсон. Тус зөвлөл нь Цагдаагийн ерөнхий газартай хамтран ажилладаг байна. Цахим орчин дахь хүүхэд, залуучуудыг хамгаалах асуудлыг “Насанд хүрээгүй хүмүүсийн интернэтийн аюулгүй орчныг бүрдүүлэх тухай хууль”, Насанд хүрээгүй хүмүүсийн аюулгүй интернэт хэрэглээг бий болгох үндсэн төлөвлөгөөг үндэслэн Дотоод хэргийн яам, Боловсрол, соёл, спорт, шинжлэх ухаан технологийн яам, холбогдох агентлагууд, Үндэсний цагдаагийн газар бусад төрийн болон хувийн байгууллагууд хамаарах бөгөөд тэдгээр нь интернэтийн аюулгүй хэрэглээний талаар сурталчлах ажлыг тогтмол зохион байгуулдаг.

- **Кибер аюулгүй байдлын стратегийн төв штаб (National center of Incidient readiness and Strategy For Cybersecutity(NISC))[459]**

2014 онд Засгийн газрын дэргэд байгуулагдан тус штаб нь кибер аюулгүй байдлын стратегийг үр дүнтэй, цогцоор нь сурталчлах, хэрэгжилтэд хяналт тавих чиг үүрэгтэй.

- **Кибер гэмт хэрэгтэй тэмцэх төв (Japan Cybercrime Control Center)[460]**

2014 онд цахим гэмт хэргийн үндэс суурийг олж тогтоох, бууруулах, саармагжуулж дараагийн учирч болох аюул ослоос урьдчилан сэргийлэх зорилгоор төр болон хувийн хэвшилтэй хамтарсан ашгийн бус байгууллага болох Японы кибер гэмт хэрэгтэй тэмцэх төв байгуулагдсан. Үйл ажиллагааны чиглэл:

- Эдийн засаг, санхүүгийн кибер гэмт хэрэг;
- Зорилтот халдлага (мэдээлэл хулгайлах);
- Цахим худалдааны платформ дээр залилан мэхлэх үйл ажиллагаа;
- Хортой програмын шинжилгээ;
- Мэдээллийн аюулгүй байдал;
- Олон улсын хамтын ажиллагаа гэсэн чиглэлтэй байна.

[459] National center of Incidient readiness and Strategy For Cybersecutity https://www.nisc.go.jp/eng/index.html
[460] Japan Cybercrime Control Center https://www.jc3.or.jp/english/

Кибер орчин дахь аюул заналхийлэл, гэмт хэргийн талаарх мэдээлэл цуглуулж дүн шинжилгээ хийх, урьдчилан сэргийлэх сургалтын хөтөлбөр боловсруулах, цогцоор нь шийдвэрлэхийн тулд цагдаагийн ерөнхий газар, мэдээлэл технологийн байгууллага, банк санхүүгийн байгууллага, хувийн хэвшлийн компани болон олон улсын хамтын байгууллагатай нягт хамтран ажилладаг байна.

- **@Police[461] цахим мэдээллийн сайт**

Үндэсний цагдаагийн газрын кибер гэмт хэрэгтэй тэмцэх хэлтсээс кибер гэмт хэрэг, кибер халдлагаас урьдчилан сэргийлэх зорилгоор ажиллуулдаг цахим мэдээллийн сайт юм.

- **Кибер аюулгүй байдлын судалгааны төв (Cybersecurity Research Institute)[462]**

Мэдээлэл, харилцаа холбоо технологийн үндэсний хүрээлэнгийн харьяа Кибер аюулгүй байдлын судалгааны төв нь нийгэмд сүүлийн үеийн тулгамдаж байгаа кибер аюулгүй байдлын талаар судалгаа шинжилгээний ажил хийдэг.

IV. Хууль эрх зүйн орчин

- **Эрүүгийн хууль (Japan Penal Code)[463]**

Энэ хууль Япон Улсын нутаг дэвсгэр болон Япон Улсын хөлөг онгоц, онгоцонд гэмт хэрэг үйлдсэн хүн бүрд адил хамаарна.

161(2) дугаар зүйл. Эрх баригч болон төрийн албан хаагчдын бүртгэл, баримтыг ашиглан бичлэг хийн олон нийтэд тараасан тохиолдолд 10 жил хүртэлх хугацаагаар хорих эсхүл 1,000,000 иений торгууль ногдуулна.

168 дугаар зүйл. Компьютерийн вирус болон буруу командын бүртгэл (Improper Command Records):

Improper Command Records гэдэг нь (a) компьютерийг операторын эсрэг ажиллуулах, буруу команд өгөх цахилгаан соронзон бичлэгийг хэлнэ.

Компьютерийн вирус болон буруу командын бүртгэл үүсгэж бусдын компьютерт вирус болон зохисгүй бичлэг тараасан этгээд болон тараахыг завдсан этгээдэд 3 жил хорих ял эсхүл 500,000 иенээр торгоно.

Hacking ажиллагаанд буруу командын бүртгэлийг ашигласан тохиолдолд 3 жил хорих эсхүл 1,000,000 иений торгууль ногдуулна.

Phishing (a) хулгайлах, залилан мэхлэх, заналхийлэх зэрэг хууль бус аргаар ажил олгогчийн худалдааны нууцыг олж авах;

(b) худалдааны нууцыг ашиглах, бусдад задруулсан тохиолдолд 10 жилийн хорих ял шийтгэл эсхүл 20,000,000 иений торгууль ногдуулна.

175(1) дүгээр зүйл. Электромагнет бичлэг агуулсан бүдүүлэг ичгүүргүй агуулгатай бичлэг үзүүлэх:

[461] @Police https://www.npa.go.jp/cyberpolice/english/index.html
[462] Cybersecurity Research Institute https://www.nict.go.jp/en/csri/
[463] Japan Penal Code http://www.isc.meiji.ac.jp/~sumwel_h/Codes/comp-crim.htm

Олон нийтэд ичгүүргүй бүдүүлэг баримт, зурмал зураг, электромагнет бичлэг бүхий эсхүл бусад агуулга бүхий мэдээлэл бичлэгээр хангасан эсхүл үзүүлсэн этгээдийг 2-оос илүүгүй жилээр хорих, эсхүл 2,500,000-аас ихгүй иенээр торгоно. Бүдүүлэг электромагнетик бичлэг эсхүл теле харилцаагаар дамжуулсан өөр бусдад бичлэг түгээсэн этгээдийг мөн адил шийтгэнэ.

3үйл 3(1)-ийн *заалтаар учрах хохирлоос урьдчилан сэргийлэх тухай*

Танихгүй хүмүүст эсхүл хэд хэдэн хүмүүст хувийн бичлэгийг теле харилцааны шугамаар дамжуулж, улмаар гуравдагч этгээд тухайн дүрс бичлэг дэх хүнийг оноон таньсан тохиолдолд тухайн бичлэг дамжуулсан этгээдийг 3-аас илүүгүй жилээр хорих эсхүл 500,000-аас ихгүй иенээр торгож шийтгэнэ.

222 (1) дугаар зүйл. *Сүрдүүлэх*:

Бусдын амь нас, эрх чөлөө, нэр хүнд, эд хөрөнгөд заналхийлж сүрдүүлсэн этгээдийг 2-оос ихгүй жилээр хорих эсхүл 300,000-аас ихгүй иенээр торгоно.

223 (1) дүгээр зүйл. Шахалт:

Бусдын амь нас, эрх чөлөө, нэр хүнд, эд хөрөнгийг доромжлол, хэрцгийлэл хэрэглэж бусдаар үйл үйлдүүлэх, эсхүл бусдыг өөрийн зүй ёсны эрхээ эдлэхэд нь саад болох зэргээр заналхийлж сүрдүүлсэн этгээдийг 3-аас илүүгүй жилээр хорьж шийтгэнэ.

230 (1) дүгээр зүйл. Гүтгэлэг:

Олон нийтийн өмнө баримт дэлгэн мэдүүлж бусдыг гүтгэсэн этгээдийг, тухайн баримт үнэн, худлаас үл шалтгаалан, 3-аас илүүгүй жилээр хорих эсхүл ажил алба эрхлүүлэхгүй байх, эсхүл 500,000-аас ихгүй иенээр торгоно.

231 дүгээр зүйл. Гутаан доромжлох:

Бусдыг олны өмнө гутаан доромжилсон этгээдийг хэдий тэр нь ямарваа баримт нотолгоо болохгүй байсан ч хөдөлмөрлөх эрхийг хасаж, жижиг гэмт хэргийн нөхцөлөөр хорих эсхүл бага хэмжээний торгууль ногдуулна.

233 дугаар зүйл. Бизнест саад учруулах:

Буруу худал цуурхал тараах эсхүл залилан мэхлэх арга замаар бусдын бизнесийн нэр хүндийг сэвтүүлэх, эсхүл саад учруулсан бол 3-аас илүүгүй жилээр хорих эсхүл 500,000-аас ихгүй иенээр торгох шийтгэл ногдуулна.

Эрүүгийн хуулийн нэмэлт өөрчлөлт

234(2) дугаар зүйл. Компьютерийн програмыг санаатайгаар гэмтээж, операторын эсрэг ашиглах, бусдын бизнест хохирол учруулах, хуурамч мэдээлэл өгөх, зохисгүй Програм суулгасан тохиолдолд 5 жил хорих эсхүл 1,000,000 иений торгууль ногдуулна.

246(2) дугаар зүйл. Хуурамч мэдээллээр бичлэг хийх, эсхүл гуравдагч этгээдийн боловсруулсан бүртгэлээр санхүүгийн ашиг олсон тохиолдолд 10 хүртэлх хугацаагаар хорих ял шийтгэнэ.

- **Хүүхдийн биеэ үнэлэх, хүүхдийн порно үйлдэлд хариуцлага ногдуулах болон хүүхдийг хамгаалах тухай хууль (Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children)[464]**

Энэхүү хуулиар хүүхдийн эрхийг илтэд зөрчсөн садар самууныг сурталчилсан болон хүүхдийг садар самуун, биеэ үнэлэх, эрүүгийн хариуцлага ногдуулах, хүүхдийн эрхийг хамгаалах үндсэн зорилготой. Мөн хуулиар интернэтээр насанд хүрээгүй хүмүүсийн порно бичлэг тараасан, бичлэг үйлдсэн этгээдэд хүлээлгэх хариуцлагыг хуульчилсан. байна.

7(6) дугаар зүйлтэй холбогдох хууль журам, шийтгэлийн тухай

Насанд хүрээгүй хүмүүс буюу 18 нас хүрээгүй хүмүүс биеэ үнэлсэн бол 5-аас дээшгүй жил хорих ял оноох, эсхүл 5 саяас ихгүй иенээр торгох ял ногдуулна. Харин хүүхдийн порно бичлэгийг тараасан этгээдэд мөн адил ял ногдуулахаар заажээ.

- **Насанд хүрээгүй хүмүүсийн интернэтийн аюулгүй орчныг бүрдүүлэх тухай хууль(Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People)[465]**

Тус хуулийг 2008 онд баталсан бөгөөд хуулиар насанд хүрээгүй буюу 18-аас доош насны хүмүүст интернэтийг зохистой ашиглах чадварыг эзэмшүүлэх, шүүлтүүрийн тархалтыг дэмжих замаар насанд хүрээгүй хүмүүсийн хортой агуулга бүхий мэдээллийг үзэх боломжийг багасгах, иргэдэд интернэтийн зохистой хэрэглээг зохицуулах үүргийг ногдуулж, түүнийг төр засгаас дэмжих бодлогыг баримталсан. Мөн холбогдох засаг захиргаа, интернэттэй холбоотой бизнес эрхлэгчид, эцэг эхчүүд, асран хамгаалагчдад хүүхдийг хор хөнөөлтэй мэдээллээс хамгаалах арга хэмжээ авах (интернэтийн зохистой хэрэглээний талаар сурталчлах, боловсрол олгох, хүүхдийн хэрэглэж буй цахим төхөөрөмжид шүүлтүүр хэрэглэж буй эсэхэд хяналт тавих гм) үүрэг хариуцлагыг ногдуулах болсон байна.

Насанд хүрээгүй хүүхдийн асран хамгаалагч хортой мэдээллийг шүүгч үйлчилгээг ашиглахгүй гэсэн хүсэлт гаргаснаас бусад тохиолдолд цахим төхөөрөмж үйлдвэрлэгч, үйлчилгээ эрхлэгчдээс шүүгч програмыг ашиглахад хялбар байдлаар суурилуулж тухайн бүтээгдэхүүнийг борлуулах, үйлчилгээ үзүүлэх үүрэгтэй. Энэхүү үүргээ биелүүлээгүй тохиолдолд заавал биелүүлэхийг шаардах эрхтэй.

Хуульд зааснаар цахим орчин дахь хүүхдийн эрхийг хамгаалах бодлогыг хэрэгжүүлэх үйл ажиллагааг “Цахим орчинд насанд хүрээгүй хүмүүст аюулгүй мэдээллийн орчныг бүрдүүлэх хороо” хариуцахаар заасан байна.

Энэ хуулийн гол зорилго нь хүүхдэд сөргөөр нөлөөлөх мэдээллээс урьдчилан сэргийлэх, шүүгч Програм хангамжийг өргөн нэвтрүүлэх боломжийг бий болгох, ингэснээр хүүхдүүдийг цахим гэмт хэргийн золиос болохоос урьдчилан сэргийлэх ач холбогдолтой юм.

[464] Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children https://antislaverylaw.ac.uk/wp-content/uploads/2019/08/Japan-Child-Prostitution-and-Child-Pornography-Law.pdf

[465] Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People https://www8.cao.go.jp/youth/youth-harm/law/pdf/for_english.pdf

- **Зөвшөөрөлгүйгээр компьютерт нэвтрэх тухай хууль (Act on Prohibition of Unauthorized Computer Access)[466]**

Хуулийн зорилго нь харилцаа холбооны хэрэгслээр дамжуулан компьютертой холбоотой гэмт хэргээс урьдчилан сэргийлэх, компьютерт зөвшөөрөлгүй нэвтрэх үйлдлийг хориглох, түүнд авах арга хэмжээ болон оногдуулах шийтгэл зэргээр харилцаа холбооны дэг журмыг сахин биелүүлэхэд оршино.

3 дугаар зүйл. Бусдын компьютерт зөвшөөрөлгүй нэвтрэх заалтыг зөрчсөн тохиолдолд гурван жил хүртэлх хугацаагаар хорих;

4 дүгээр зүйл. Хэрэглэгчийн таних кодыг зөвшөөрөлгүй авсан тохиолдолд нэг жил хүртэлх хугацаагаар хорих, эсхүл 500,000 иенээр торгох;

5 дугаар зүйл. Хэрэглэгчийн таних кодыг админ, эсхүл гуравдагч этгээдэд дамжуулсан тохиолдолд 300,00 иенээр торгох;

6 дугаар зүйл. Хууль бусаар олж авсан хэрэглэгчийн таних кодыг хадгалах;

7 дугаар зүйл. Администраторын дүр эсгэх;

(a) Хуурамч администраторааc хэрэглэгчийг таних кодоо оруулахыг хүссэн вэбсайт үүсгэх;

(b) Хуурамч администраторааc хэрэглэгчийг таних кодоо оруулахыг хүссэн цахим шуудан илгээсэн тохиолдолд нэг жил хүртэлх хугацаагаар хорих эсхүл 500,000 иений торгууль ногдуулна.

Хакердах – 3 жил хүртэл хугацаагаар хорих эсхүл 1,000,000 иений торгууль ногдуулна.

- **Кибер аюулгүй байдлын тухай хууль(The Basic Act on Cybersecurity)[467]**

Мэдээллийн чөлөөт урсгалыг хангах, кибер аюулгүй байдлыг хамгаалах энэхүү хуулийн зорилго нь кибер аюулгүй байдлын бодлого:

- Үндэсний кибер аюулгүй байдлын зарчмуудыг тусгах;
- Засгийн газар, орон нутгийн засаг захиргаа болон бусад холбогдох олон нийтийн байгууллагын үүрэг хариуцлагыг тодорхой болгох;
- Кибер аюулгүй байдлын стратегийг боловсруулж кибер аюулгүй байдалтай холбоотой бодлогод зайлшгүй шаардлагатай зүйлийг тодорхойлох;
- Мэдээлэл, харилцаа холбооны дэвшилтэт сүлжээ нийгэмлэг байгуулах тухай үндсэн хууль (2000 оны 144 тоот хууль)-ийн хамт кибер аюулгүй байдлын стратегийн төв штаб байгуулснаар ард түмний аюулгүй байдал, аюулгүй нийгэмд амьдрах боломжтой нөхцөлийг бүрдүүлэх, олон улсын энх тайван, аюулгүй байдал, үндэсний аюулгүй байдлыг хамгаалахад хувь нэмэр оруулахад оршино.

18 дугаар зүйл. Засгийн газар кибер гэмт хэргийг таслан зогсоох, хохирлоос урьдчилан сэргийлэх үүрэгтэй.

[466] Act on Prohibition of Unauthorized Computer Access
http://www.japaneselawtranslation.go.jp/law/detail_main?re=01&vm=02&id=2250
[467] The Basic Act on Cybersecurity
http://www.japaneselawtranslation.go.jp/law/detail/?printID=&re=02&vm=02&id=2760&lvm=01

4.5 ГЕРМАН УЛС

I. Цахим орчин дахь гэмт хэргийн нөхцөл байдал[468]

2020 онд Герман Улсад 108,474 кибер гэмт хэрэг бүртгэгдсэн нь 2019 оныхоос 7.9%-иар, 2015 оныхоос 2 дахин нэмэгдсэн байна. Хүүхэд залуучуудыг цахим орчин дахь хүчирхийллээс хамгаалах үйл ажиллагаа, хяналтыг явуулдаг Jungendschutz.net цахим хуудсанд бүртгэгдсэн 7513 зөрчлийн ангиллыг авч үзэхэд хүүхдийг садар самуунд уруу татах гэмт хэрэг 41%-ийг эзэлж байгаа бол улс төрийн хэт туйлшралтай холбоотой цахим гэмт хэрэг, порнографтай холбоотой, хүүхэд залууст хор хөнөөлтэй мэдээлэл зэрэг нь бусад хувийг эзэлж байна. Эдгээр цахимаар үйлдэгдсэн гэмт хэргийн 86% нь гадаадын серверээс ирсэн бөгөөд агуулгын тал орчим хувь нь платформ дээр илэрчээ. Ялангуяа Facebook (14%), YouTube (10%), Twitter (6%), Instagram (5%), Tumblr (4%) нар ихээхэн хувийг эзэлж байжээ. Хор хөнөөлтэй мэдээллийг устгах амжилтын хувь нь дотоодын сервер дээр 100%, гадаадын серверүүдийн хувьд 92% байна. Хугацааны хувьд Германд дунджаар 4,8 хоногийн хугацаанд устгадаг бол гадаадын серверүүд 7,8 хоногт устгадаг байна.

Европын Холбооноос жил бүрийн 10 сарыг “Кибер аюулгүй байдлын сар” (CyberSecMonth)[469] болгон зарлаж иргэд болон байгууллагад кибер аюулгүй байдлыг сурталчлах, сайн туршлагыг нэвтрүүлэх, хуваалцах замаар онлайн аюулгүй байдлын хамгийн сүүлийн үеийн мэдээллээр хангадаг байна. 2021 онд Кибер анхны тусламж, Гэртээ хэрхэн кибер аюулгүй байдлыг хангах вэ гэсэн сэдэвтэй байна.

II. Цахим орчин дахь гэмт хэргийн стратеги төлөвлөгөө

Цахим гэмт хэргээс урьдчилан сэргийлэх зорилгоор Герман Улсын Засгийн газар болон Эрүүгийн цагдаагийн газар, иргэний нийгэм, хувийн секторууд ба олон улсын байгууллагуудын хамтын ажиллагааны хэлбэрээр маш өргөн цар хүрээтэй санал санаачилгуудыг гарган, дэмжих бодлогыг баримтлан ажилладаг. Энэ хүрээнд хууль эрх зүйн орчныг боловсронгуй болгох, хэрэгжилтэнд хяналт тавих, бодлого хөтөлбөр боловсруулах, хүүхэд залууст мэдлэг олгох, цахим орчныг ашиглах боловсролыг дээшлүүлэх, мэдээ мэдээллээр хангах, цахим гэмт хэрэг, хүчирхийллээс хамгаалах арга хэрэгслийг нэвтрүүлэх зэрэг өргөн хүрээний цогц арга хэмжээг авч ирсэн байна. Тухайлбал:

- ***Кибер аюулгүй байдлын стратеги 2021***[470]

  Холбооны Засгийн газрын тогтоолоор 2011, 2016 онд кибер аюулгүй байдлын стратеги төлөвлөгөөг батлан хэрэгжүүлж ирсэн. Энэ удаагийн 2021 оны стратеги төлөвлөгөөнд:

  1. Төрийн байгууллага, бизнес, нийгэм, шинжлэх ухааны хамтын хариуцлагаар цахим аюулгүй байдлыг бүрдүүлэх;
  2. Төр, бизнес, шинжлэх ухаан, нийгмийн цахим халдашгүй байдлыг бэхжүүлэх;
  3. Цахим хөгжлийн аюулгүй байдлыг хангах;
  4. Хэмжигдэхүйц хийгээд ил тод болгох гэсэн 4 чиглэлийн дагуу хэрэгжүүлнэ.

[468] Children on the Internet https://www.jugendschutz.net/fileadmin/download/pdf/Report_2019_Children_on_the_Internet.pdf
[469] European Cybersecurity Month 2021 https://www.nixu.com/
[470] CyberSecurity Strategy for Germany 2021 https://www.bundesregierung.de/breg-en/news/new-cyber-security-strategy-1958688

- ***Райнландын 10 зүйлт хөтөлбөр*** (Rhineland's 10 Point Program)- Интернэтийн зохистой хэрэглээний талаарх мэдлэгийг дээшлүүлж, суурь мэдлэгтэй болгох замаар хүүхэд, залуучуудыг аюултай цахим агуулгаас хамгаалах зорилготойгоор боловсруулж 2007 оноос хэрэгжүүлсэн. Энэхүү хөтөлбөр нь Европын Холбооноос санхүүждэг Киксейф (Kicksafe) зэрэг хөтөлбөрүүдтэй хамтран ажилладаг.
- ***Киксейф хөтөлбөр*** (Kicksafe)- Мөн хүүхэд, залуучуудын интернэт болон цахим хүчирхийллийн талаарх ухамсар, мэдлэгийг дээшлүүлэх зорилготойгоор 2009 оноос хэрэгжүүлж эхэлсэн. Хөтөлбөр нь хүүхэд, залуучуудыг өөрийн “хүүхэд залуучуудын” цахим хуудсаар дамжуулан нэгтгэж, шинээр тулгамдаж буй асуудлуудыг танилцуулдаг. Энэ хөтөлбөрийн хүрээнд жил бүрийн 2 дугаар сарын 5-ны өдрийг Европын “*Илүү аюулгүй интернэтийн өдөр*” болгон тэмдэглэдэг ба засгийн газрын болон хувийн хэвшлийн олон байгууллагуудтай хамтран ажиллаж, интернэт орчны аюулгүй байдал ба цахим хүчирхийллийн талаарх мэдээллүүдээр хангадаг. Европын Холбооны хэмжээнд улс орон тус бүрийн онцлог асуудлыг хөндөн үзэх үүднээс тусгайлсан цахим сүлжээнүүдийг бий болгон ажиллуулдаг байна.
- ***Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM)*** буюу Сайн дурын өөрийгөө зохицуулах мультимедиа үйлчилгээ үзүүлэгчдийн ассоциаци нь хүүхэд залуучуудыг аюултай цахим агуулгаас хамгаалах зорилгоор 1997 онд үүсгэн байгуулагдсан бөгөөд хууль бус болон аюултай цахим агуулгын талаарх мэдээг шинжлэн үздэг (Hotline)-ыг ажиллуулдаг. FSM нь 1999 онд INHOPE нэртэй интернэтийн хотлайн ажиллуулагчдын Олон улсын ассоциацийг бусадтай хамтран үүсгэн байгуулсан ба энд ихэвчлэн Европт байрлах 20 гаруй интернэтийн хотлайн нэгдэн орсон байна. INHOPE нь интернэтийн аюулгүй байдлыг ханган ажилладаг Hotline ажиллах орчныг нөхцөлдүүлж, хамтран ажилладаг.
- ***Интернэт ба Дижитал Нийгмийн лавлах***- Дижитал ур чадвар, боловсролыг дээшлүүлэх чиглэлээр зөвлөгөө өгч, гарын авлагаар ханган ажилладаг. Энд бас муж улсын түвшинд үйл ажиллагаа явуулдаг “Medienpass NRW” хөтөлбөр (хэвлэл мэдээллийн сувгийн паспорт) зэргийг дурдаж болно.

III. Холбогдох байгууллагууд

Цахим болон нийгмийн сүлжээн дэх аливаа гэмт хэрэг, халдлагаас ард иргэдийг хамгаалах үйл ажиллагааг Холбооны Хууль зүйн яам, Гэр бүлийн яам, Цагдаагийн байгууллага, Эрүүгийн цагдаагийн газар хариуцахаас гадна Гэр бүлийн яамны харьяа Хүүхэд, залуучуудад хортой мэдээллийн хяналтын холбооны зөвлөл (BPJM), Цахим орчин дахь хүүхэд, залуучуудыг хамгаалах комисс (KJM) зэрэг байгууллагууд хариуцан ажилладаг. Эдгээр төрийн захиргааны байгууллагууд нь Хүүхэд, залуучуудыг хамгаалах хууль, Нийгмийн сүлжээн дэх хүүхэд, залуучуудын хамгааллын тухай муж хоорондын гэрээ зэрэг эрх зүйн орчны хүрээнд үйлчилгээ үзүүлэгч байгууллагуудын үйл ажиллагааг хянах, мэдээллийг индексжүүлэх, гомдол хүлээн авах, шийдвэрлэх, хүүхдийн цахим хүчирхийллийн эсрэг хөтөлбөр, үйл ажиллагаа хэрэгжүүлэх зэргээр хяналт тавьдаг.

- ***Эрүүгийн цагдаагийн газар (Bundeskriminalamt)[471]***

  Эрүүгийн цагдаагийн газар нь улс төрийн зорилготой гэмт хэрэг, терроризм, хар тамхитай холбоотой гэмт хэрэг, цахим гэмт хэргийг хариуцан ажилладаг. Эрүүгийн цагдаагийн газрын харьяа Кибер гэмт хэрэгтэй тэмцэх хэлтэс нь дотроо гэмт хэргийн талаар мэдээлэл цуглуулах төв, үйл ажиллагаанд дүн шинжилгээ хийх төв, судалгааны төв, хүүхэд, өсвөр үеийнхний гэмт хэрэгтэй тэмцэх төв гэсэн нэгжүүдтэй байна.
- ***Холбооны Гэр бүлийн яам (Federal Ministry for Family Affairs)[472]***

  Цахим болон нийгмийн сүлжээн дэх хүчирхийллийн аливаа гэмт хэрэг, халдлагаас хүүхэд, залуу үеийг хамгаалах үйл ажиллагааг Холбооны гэр бүлийн яам хариуцахаас гадна тус яамны харьяа Хүүхэд, залуучуудад хортой мэдээллийн хяналтын холбооны зөвлөл (BPJM)[473], Цахим орчин дахь хүүхэд, залуучуудыг хамгаалах комисс (KJM)[474] газар зэрэг байгууллагууд хариуцан ажилладаг. Эдгээр төрийн захиргааны байгууллагууд нь Хүүхэд, залуучуудыг хамгаалах хууль, Нийгмийн сүлжээн дэх хүүхэд, залуучуудын хамгааллын тухай муж хоорондын гэрээ зэрэг эрх зүйн орчны хүрээнд үйлчилгээ үзүүлэгч байгууллагуудын үйл ажиллагааг хянах, мэдээллийг индексжүүлэх, гомдол хүлээн авах, шийдвэрлэх, хүүхдийн цахим хүчирхийллийн эсрэг хөтөлбөр, үйл ажиллагаа хэрэгжүүлэх зэргээр хяналт тавьдаг. Мөн эдгээр нь Холбооны хууль зүйн яам, Германы цагдаагийн байгууллага, төрийн болон хувийн, олон нийтийн байгууллагуудтай нягт хамтран ажилладаг байна.
- ***Цахим орчин дахь хүүхэд, залуучуудыг хамгаалах комисс (The Commission for the Protection of Minors in the Media)[475]***

  Интернэтийн нэвтрүүлгийг байнга хянах төв захиргаа нь агуулга нийтлэн түгээгч нарыг залуучуудыг хамгаалах хууль эрх зүйд нийцүүлэн ажиллах явдлыг баталгаажуулдаг төрийн хэвлэл мэдээллийн зохицуулагч байгууллага юм. Тус Комисс нь хууль журам зөрчигдсөн эсэхийг тодорхойлж, удирдан чиглүүлэх арга хэмжээний шийдвэрийг гаргана. Тухайн нэг агуулгыг хориглох эсхүл торгууль ногдуулах гэхчлэн зөрчлийн хүнд, хөнгөн хэлбэрийн хэмжээнээс хамааран харилцан адилгүй янз бүрийн хуулийн хариуцлагыг ногдуулна. Үүнд, тухайн нийтлэл, агуулга түгээгчийн харьяа мужийн хэвлэл мэдээллийн захиргаа нь зохих арга хэмжээг авч хэрэгжүүлэх үүрэгтэй.
- ***Телефон зөвлөгөө, үйлчилгээний төв (Nummer gegen Kummer)[476]***

  Хүүхэд сэтгэлийн дарамтад орох үедээ залгаж тусламж авах боломжтой “Хүүхэд, залуучуудад туслах шугам (“Nummer gegen Kummer”) буюу Телефон зөвлөгөө, үйлчилгээний төвийн 116 111 утасны дугаарыг ажиллуулдаг. Энд өдөрт дунджаар хоёр дуудлага тутмын нэг нь цахим хүчирхийлэлтэй холбоотой байдаг байна.

[471] Bundeskriminalamt https://www.bka.de/EN/Home/home_node.html
[472] Federal Ministry for Family Affairs https://www.bmfsfj.de/bmfsfj/meta/en
[473] BPJM https://www.bzkj.de/bzkj/meta/en
[474] The Commission for the Protection of Minors in the Media https://www.kjm-online.de/en/
[475] The Commission for the Protection of Minors in the Media https://www.kjm-online.de/en/
[476] Nummer gegen Kummer https://www.nummergegenkummer.de/

- ***jugendschutz.net*** [477] цахим хуудас нь мужийн захиргааны зорилго, зорилтоо хэрэгжүүлэхэд нь дэмжин тусалдаг бөгөөд интернэт агуулгыг хянаж, Залуучуудыг хамгаалах хууль зөрчсөн үйлдлийг тогтоон таньж, Комисст дараагийн арга хэмжээг авхуулахаар уламжилна.
- ***Хүүхэд, залуучуудад хортой мэдээллийн хяналтын холбооны зөвлөл (The Federal Review Board for Media Harmful to Minors)*** [478] нь онлайн агуулгыг залуучуудад аюултай эсэхийг шийдэх үүрэг хүлээнэ. Зөвлөл нь бусад захиргааны байгууллагуудын албан хүсэлтээр үйл ажиллагаагаа явуулах ба “индекс жагсаалтад” URLs-уудыг оруулна. Үүнээс гадна Холбооны хянан шалгах зөвлөл нь интернэт орчинд хүүхэд, залуусыг найдвартай хамгаалахад учирч болзошгүй гэмт үйлдлүүдэд хариу арга хэмжээ авах албан ёсны эрх үүрэгтэй зөвлөл юм.

IV. Хууль эрх зүйн орчин

Тус улсын хууль эрх зүйд заасан цахим орчинд үйлдэгдэж байгаа гэмт хэргүүд нь Будапештийн конвенцтой тэр бүр шууд холбогддоггүй учраас Германд тэрхүү конвенцын бодит чадамжийг цахим гэмт хэргийг явцуу хүрээгээр авч үздэг гэж дүгнэжээ. Цахим орчин дахь гэмт хэргийг Эрүүгийн хууль болон Нийгмийн сүлжээн дэх хуулийн хэрэгжилтийг хангах тухай хууль, Теле мэдээллийн тухай хуулиар нийтлэг зохицуулдаг байна. Үүнээс гадна цахим сүлжээн дэх хүүхэд хамгааллын асуудлыг “Залуучуудыг хамгаалах тухай хууль” (JuSchG)[479] нь CD зэрэг биет мэдээллийг нийтэд түгээх асуудлыг зохицуулж, чухам алийг хүүхэд, залуучуудад хортой мэдээллийн жагсаалтад оруулахыг тодорхойлно. Мужийн түвшинд (Länder level) “Нийгмийн сүлжээн дэх хүүхэд, залуучуудын хамгааллын тухай муж хоорондын гэрээ”[480] (JMStV) нь интернэт болон өргөн нэвтрүүлэгт хэрэглэгддэг цорын ганц хууль эрх зүйн үндэс юм.

- **Германы Эрүүгийн хууль (Criminal Code)**[481]

Герман Улс бусад орнуудын нэгэн адилаар цахим орчин дахь гэмт хэргийг шийдвэрлэхэд Эрүүгийн хуулийн заалтуудыг хэрэглэж байна. Тухайлбал, Хууль бус суртал ухуулгын материал тараах буюу Үндсэн хуульд харшилсан байгууллагын тэмдэглэгээг ашиглах, төрийн эсрэг онц хүнд гэмт хэрэг үйлдэхийг дэмжих, хууран мэхлэх гэмт хэрэг үйлдэхийг завдах, олон нийтийг гэмт хэрэгт уриалах, мөн үзэн ядахыг өөгшүүлэх болон бусад гэмт үйлдлийн тохиолдлуудад дараах Эрүүгийн хуулийн зүйл заалтуудыг хэрэглэн шийдвэрлэнэ. Үүнд:

Эрүүгийн хуулийн 202 дугаар хэсэг (a) Нэвтрэхийг хориглосон хамгаалагдсан өгөгдөлд хууль бусаар нэвтэрсэн тохиолдолд 3 жил хүртэлх хугацаагаар хорих эсхүл торгууль ноогдуулна (b)Phishing хийсэн тохиолдолд 2 жил хүртэлх хугацаагаар хорих эсхүл торгууль ноогдуулна. 263 дугаар хэсэг (компьютерийн залилан)- 5 жил хүртэлх хугацаагаар хорих эсхүл торгууль ноогдуулна. 269 дүгээр хэсэг (техникийн бүртгэлийг хуурамчаар үйлдэх), 238 дугаар хэсэг (бусдыг хууль бусаар мөшгих), 240 дүгээр хэсэг (бусдыг заналхийлэх, хүч

[477] Jugendschutz.net https://www.jugendschutz.net/en/index.html
[478] The Federal Review Board for Media Harmful to Minors https://www.bzkj.de/bzkj/Service/english.html
[479] German Law Archive https://germanlawarchive.iuscomp.org/?p=724
[480] Interstate Treaty on the Protection of minors https://www.kjm-online.de/
[481] Criminal Code (Strafgesetzbuch, StGB) https://germanlawarchive.iuscomp.org/?p=752

хэрэглэх хэлбэрээр үйл үйлдүүлэх, зовоох эсхүл эс үйлдүүлэх), 241 дүгээр хэсэг (гэмт хэрэг үйлдэхээр сүрдүүлэх), 176 дугаар зүйл (хүүхдийг хүчирхийлэх), 185 дугаар хэсэг (гутаан доромжлох), 186 дугаар хэсэг (гүтгэх), 187 дугаар хэсэг (санаатайгаар гүтгэх), 201 дүгээр хэсэг (үг ярианы хувийн нууцыг алдагдуулан зөрчих), 201а хэсэг (хувийн нууцыг зураг авч зөрчих) ба Үзүүлэх урлагийн бүтээл, фото зургийн зохиогчийн эрхтэй холбоотой хуулийн 33 дугаар хэсэг зэрэг багтана. Эрүүгийн хуулийн 238 дугаар хэсэгт (хууль бусаар мөшгих) теле харилцааны арга зам (1-р догол мөрийн 2 дугаарт) эсхүл хэн нэгний хувийн мэдээллийг ашиглах (1-р догол мөрний 3 дугаарт) зэргийг маш тодорхой заасан байдаг. Хүүхдийн хүчирхийллийг заасан 176 дугаар хэсэгт ч мөн адил теле харилцааны арга хэлбэрийг тодорхой хамруулан заасан (4-р догол мөрний 3 ба 4 дүгээрт).

- **Нийгмийн сүлжээн дэх хуулийн хэрэгжилтийг хангах тухай хууль (Network Enforcement Act)[482]**

2017 оны 6 дугаар сараас хүчин төгөлдөр мөрдөж эхэлсэн “Нийгмийн сүлжээн дэх хуулийн хэрэгжилтийг хангах тухай хууль”[483] нь Эрүүгийн хуулийн хүчин төгөлдөр үйлчилж буй заалтуудыг нийгмийн сүлжээний онцгой орчинд хэрэгжүүлэх, нийгмийн сүлжээ эрхлэгчдэд гомдол хүлээн авч барагдуулах үр өгөөжтэй, ил тод менежментийг нэвтрүүлэх үүргийг хүлээлгэх, нийгмийн сүлжээ эрхлэгчид, төрийн захиргааны байгууллагуудын мэдэгдэл, шүүхийн зарлан дуудах, шүүхийн шийдвэр хүлээн авах, тэдгээртэй харилцах түншийг нэр заан томилох зэргийг зохицуулна.

Нийгмийн сүлжээнд хуулийн хэрэгжилтийг хангах тухай хууль нь нийгмийн сүлжээ эрхлэгчдэд зориулсан хууль бөгөөд 2 саяас илүү бүртгэлтэй хэрэглэгч бүхий нийгмийн цахим сүлжээ бүрийг санал гомдлыг үр дүнтэй барагдуулах менежменттэй байхыг шаарддаг ба тодорхой цаг, хүрээнд Эрүүгийн хуулийн тодорхой зүйл заалтуудыг зөрчсөн хууль бус агуулгыг мэдэгдсэн даруйд нь устгах эсхүл хаах үүргийг хүлээнэ. Харин хувираа нийгмийн сүлжээ хэрэглэгчдэд үйлчлэхгүй.

Хуулиар нийгмийн сүлжээ эрхлэгчдэд шийдвэр гаргах тодорхой хугацааны хязгаарыг зааж өгсөн. Мөн нийгмийн сүлжээ эрхлэгчдээс хэрэглэгчдийн гомдлыг хүлээн авч барагдуулах хандалтын аливаа саадгүй, ойлгомжтой, ил тод аргачлалыг нэвтрүүлэхийг шаарддаг учраас үйлчилгээ эрхлэгчид тэдний платформ дээр Германы эрүүгийн хууль зөрчсөн байж болзошгүй агуулгын талаар мэдээлэл өгөхөд ашиглах ойлгомжтой, хялбар боломжийг хэрэглэгчдэд олгох ёстой. Нийгмийн сүлжээ эрхлэгчид эдгээр мэдээллийг хүлээн авмагц нэн даруй хуулиар тогтоосон хугацаанд багтаан боловсруулж гаргасан шийдвэрээ танилцуулах ёстой.

Хэрвээ нийгмийн сүлжээ эрхлэгчид хуулиар ногдуулсан үүрэг болох гомдол хүлээн авч барагдуулах менежментийг нэвтрүүлээгүй, хугацаа хэтрүүлсэн, эсвэл Германы эрүүгин хуулийн зохих заалтуудын дагуу агуулгыг устгах, хаах үүргээ үл тоомсорлосон бол 5 сая хүртэлх еврогийн мөнгөн торгууль төлөх, онц ноцтой тохиолдолд 50 сая хүртэлх еврогийн торгууль төлөх юм.

[482] Үзэл бодлоо чөлөөтэй илэрхийлэх зааг хязгаар. Фрейдрих Эбертийн сан. 2018 он. http://library.fes.de/pdf-files/bueros/mongolei/14077.pdf

[483] Network Enforcement Act https://germanlawarchive.iuscomp.org/?p=1245

Нийгмийн сүлжээ эрхлэгчид хууль зүй, төрийн захиргааны байгууллагууд болон иргэдийн зүгээс агуулгын болон бусад асуудлаар хандаж байх байнгын түншийг нэр заан томилох үүргийг хүлээнэ. Тухайн түншид хандсан асуултад 48 цагийн дотор хариу өгөх ба хугацаа хэтрүүлсэн тохиолдолд мөнгөн торгууль ногдуулна.

Хуулийн хэрэгжилтэд хяналт тавих, мөнгөн торгууль ногдуулах, нийгмийн сүлжээ эрхлэгчдийн талаар иргэдийн гаргасан гомдлыг Холбооны Хууль зүй, Хэрэглэгчдийн эрхийг хамгаалах яамны харьяа Холбооны хууль зүйн газар хариуцна.

Энэхүү хууль батлагдсантай холбоотойгоор **Теле мэдээллийн хэрэгслийн тухай хуульд** өөрчлөлт оруулж (интернэтийг зохицуулах суурь хууль) онц ноцтой тохиолдолд нийгмийн сүлжээ эрхлэгчдэд хууль зөрчсөн агуулгын зохиогчийн мэдээллийг ил болгох үүргийг ногдуулах эрхийг шүүхэд олгосон. Тухайлбал, доромжлуулсан иргэн зохиогчийг иргэний шүүхэд өгч болно. Ингэснээр доромжлолд өртсөн хүн нийгмийн сүлжээнд тухайн иргэнийг доромжилсон, гүтгэсэн агуулга нийтлүүлснийх нь төлөө зохиогчоос хохирлын мөнгө төлүүлэх боломж бүрдсэн байна.

Мөн Нийгмийн сүлжээнд хуулийн хэрэгжилтийг хангах тухай хууль ёсоор нийгмийн сүлжээ эрхлэгч компаниуд хагас жил тутамд тайлан гаргах ёстой байдаг байна. Тус хуулийн үндсэн ач холбогдол нь зөвхөн иргэд болон байгууллагууд, төрийн захиргааны байгууллагуудын зүгээс мэдээлэл ирсэн тохиолдолд уг мэдээллийг үндэслэн тухайн агуулгын мөн чанар, түүнтэй холбоотойгоор тухайн агуулгыг устгах, хаах тухай шийдвэрийг эхлээд нийгмийн сүлжээ эрхлэгчид гаргадагт оршино. Тийм учраас энэ хууль нь нийгмийн цахим сүлжээнд эрүүл зөв орчныг бүрэлдүүлэх, цахим дарамт шахалт болон онлайн хүчирхийллийг зогсооход чухал хувь нэмэртэй байгаа ажээ. (*энэ хууль батлагдсанаар Фэйсбүүк компани гэхэд л Герман улсад өөрийн гэсэн 2 контент устгалын төвийг байгуулаад байгаа ба тэр нь 1200 ажилтантайгаар хяналт шалгалтын үйл ажиллагааг 24 цагаар явуулж байна. Хэрэв тус контент устгалын төв Герман Улсын нутаг дэвсгэр дээрх Фэйсбүүкийн хэрэглээ, контентод байнгын хараа хяналт тавих ба ямар нэгэн зөрчилтэй контент илэрвэл түүнийг нь 24 цагийн дотор устгах үүрэгтэй.*)

Хүүхэд, залуучуудад аюултай агуулга гэдэгт жишээлбэл насанд хүрэгчдийн порно эсхүл “Хүүхэд, залуучуудад хор хөнөөлтэй мэдээлэл” гэх жагсаалтад (индекс жагсаалт) орсон агуулгуудыг тооцох ба эдгээрийг зөвхөн насанд хүрэгчдэд л үзүүлж болно. Энэ агуулгад хүүхэд, залуучууд нэвтрэх явдлыг хаах үүднээс цахим сүлжээгээр хангагч нар шаардлага хангахуйц түвшний “нас тогтоох системийг” (age verification system)-ийг нэвтрүүлэн ашиглах ёстой. Мөн маш их бухимдал, айдсыг төрүүлэхүйц *хортой агуулгад* нэвтрэх хязгаарлалтыг үзэхэд мөн тодорхой хязгаарлалтыг хийх шаардлагыг цахим сүлжээ эрхлэгчдэд тавина. Үүний тулд KJM-ээс хүлээн зөвшөөрсөн нэвтрэх техникийн хамгаалалтын арга хэмжээнүүдийг (technical protection measures) авч хэрэгжүүлнэ. Мөн телевизороор хязгаарлалт тогтоосон зэрэглэлийн дагуу цацаж болно (жишээлэхэд,16 дугаар зэрэглэлийн агуулгыг 22 цагаас хойш үзүүлэх гэх мэт).

Зар сурталчилгаатай холбоотой тусгай журмууд бий: зар сурталчилгаа түгээгчид хүүхэд багачуудын гэнэн, туршлагагүй байдлыг ашиглан ямар нэг бүтээгдэхүүн, эсхүл үйлчилгээг худалдан авахыг шууд хандан сурталчилж болохгүй.

Энэ мэтчилэн дээрх хуулийн олон салбар хүрээ нь цахим дарамт шахалт ба цахим хүчирхийллээс урьдчилан сэргийлэхтэй холбогдож байдаг. Эрүүгийн хууль болон эдгээр хуулиас гадна Иргэний хууль (нөхөн төлбөр, арилгах ба хориглох), Хөдөлмөрийн хууль (сануулах хуудас), Цагдаагийн хууль ба Үйлчилгээ үзүүлэгчдийн журам зэргийг багтаасан захиргааны хууль зэрэгт холбогдох зүйл заалтууд бий. Тухайлбал, **Иргэний хуулийн** хүчирхийлэл ба мөшгөх үйлдлээс урьдчилан сэргийлэх заалтууд нь шүүхэд цаашдын урьдчилан сэргийлэх арга хэмжээг авах үндэслэл болдог байна.

4.6 ИХ БРИТАНИ, УМАРД ИРЛАНДЫН НЭГДСЭН ХААНТ УЛС

I. Цахим орчин дахь гэмт хэргийн нөхцөл байдал

ИБУИНХУ-д цахим гэмт хэрэг нь цар хүрээ нь нэмэгдэж, хувь хүмүүсийг эрүүл мэнд болон эдийн засгийн хувьд хохироох, аюул, эрсдэлд оруулахаас эхлээд улс орны нийгэм, эдийн засгийн чухал суурь дэд бүтэц, зайлшгүй шаардлагатай төрийн болон хувийн хэвшлийн аж ахуйн нэгж, байгууллагуудын үйл ажиллагааг тасалдуулах, доголдуулах, цаашлаад үндэсний аюулгүй байдалд заналхийлэх хэмжээний хэргүүд цахимаар үйлдэгдэж, тооцож баршгүй хохирол учруулдаг байна. Хувь хүн болон байгууллагууд нь аюулгүй байдлаа хангаагүйн улмаас цахим гэмт хэрэг үйлдэгсдийн өгөөш болсоор байна. Гэмт хэрэгтнүүд нууц үг, баримт мэдээлэл зэргийг хулгайлж гэмт хэрэгтээ ашиглахаас гадна банкны данснаас шууд мөнгө хулгайлах зэргийг цахимаар үйлдэж байна. Цахимаар хамгийн их үйлдэгдэж буй гэмт хэргийн төрлүүдэд:

- Нийгмийн сүлжээ болон цахим шуудангийн нууц үг ашиглан хакердах
- Хуурамч цахим шуудан ашиглан аюулгүй байдлын мэдээлэл, хувийн мэдээлэл авах (phishing)
- Хортой Програм хангамж-гэмт хэрэгтнүүд файлуудыг хулгайлж компьютерийн систем болон сүлжээнд халдах (malicious software)
- Мөнгө хулгайлах зорилгоор цахим хуудас руу халдах ингэхдээ тухайн цахим хуудасны сүлжээ болон серверийг хэт их ачааллах замаар үйлдэх (Distributed denial of service) зэрэг ордог байна.

II. Цахим орчин дахь гэмт хэргийн стратеги төлөвлөгөө

Тус улс нь 5 жил тутам “Үндэсний Цахим Аюулгүй байдлын Стратеги” (National Cyber Security Strategy)-ийг шинэчлэн боловсруулж, баталдаг байна.[484] Тус стратеги нь ИБУИНХУ-ын цахим орчны аюулгүй байдлыг дотооддоо болон гадаад орчинд хамгаалахад Засгийн газраас авч хэрэгжүүлэх үйл ажиллагааны төлөвлөгөө юм. 2016-2021 онд цахим орчны аюулгүй байдлыг хамгаалах Хэрэгжилтийн төлөвлөгөө нь (Implementation plan):

- **Хамгаалах**
  - Идэвхтэй цахим хамгаалалтыг бий болгох;
  - Илүү найдвартай интернэт холбоо харилцааг бий болгох;
  - Засгийн газрыг хамгаалах;

[484] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

- Үндэсний чухал дэд бүтцийн байгууламжууд болон бусад тэргүүлэх салбаруудаа хамгаалах;
- Олон нийтийн болон бизнес эрхлэгчдийн хандлагыг өөрчлөх;
- Гэмт хэргийг шийдвэрлэх, цахим аюулын талаарх ойлголтыг нэмэгдүүлэх.

- **Урьдчилан сэргийлэх**
  - Урьдчилан сэргийлэх үйл ажиллагаан дахь цахим орчны үүрэг;
  - Цахим гэмт хэргийг бууруулах;
  - Бусад улс орны цахим гэмт хэрэгтнүүдтэй тэмцэх;
  - Терроризмоос урьдчилан сэргийлэх;
  - Цахим хариу арга хэмжээний чадавхыг нэмэгдүүлэх;
  - Криптографыг нэмэгдүүлэх.

- **Хөгжүүлэх**
  - Цахим аюулгүй байдлыг хамгаалах ур чадварыг бэхжүүлэх;
  - Цахим аюулгүй байдлын салбарыг өргөжүүлэх;
  - Цахим аюулгүй байдлын салбар дахь шинжлэх ухаан, технологийн дэвшлийг дэмжих зэрэг 3 цогц үйл ажиллагаанаас бүрдэж байна.

III.Цахим гэмт хэрэгтэй тэмцэх байгууллагууд

Үндэсний Гэмт хэрэгтэй тэмцэх агентлаг (National Crime Agency)[485] нь үндэсний хэмжээнд цахим болон бусад төрлийн гэмт хэрэгтэй тэмцдэг байна.

Цахим гэмт хэрэг нь дэлхий нийтийг хамарсан аюул болоод байгаа учир олон улсын байгууллагууд, улс орнууд хоорондын хамтын ажиллагаа зайлшгүй шаардлагатай байна. Тус улсын Үндэсний Гэмт хэрэгтэй тэмцэх агентлаг нь ИБУИНХУ-ын Цагдаагийн газар, бүсийн зохион байгуулалттай гэмт хэрэгтэй тэмцэх нэгжүүд, олон улсын хууль сахиулах байгууллагууд, тухайлбал, Европын Холбооны Мөрдөх товчоо, АНУ-ын Тагнуулын алба зэрэгтэй мэдээ мэдээллээ хуваалцан хамтарч ажиллахын зэрэгцээ хувийн хэвшлийнхэнтэй техникийн туршлагаа хуваалцан, үр дүнтэйгээр хамтран ажилладаг байна.

Түүнчлэн иргэд, олон нийт, бизнес эрхлэгчдийг цахим халдлагаас урьдчилан сэргийлэх зорилгоор төрийн болон төрийн бус байгууллагуудтай хамтарч ажилладаг. Үүнд: Үндэсний Цахим Аюулгүй байдлын төв (National Cyber Security Centre)[486], тус төвийн харьяа зөвлөгөө өгөх төв, Аюулгүй интернэт хэрэглээний талаар мэргэжилтний зөвлөгөө өгөх төв (Get Safe Online Free expert advice)[487] зэрэг олон байгууллагууд багтана.

Үндэсний гэмт хэрэгтэй тэмцэх агентлаг нь цахим орчинд гэмт хэрэг үйлдэгч өсвөр насныхан болон залуучуудыг цахим хэрэгтэн болохоос сэргийлж, тэдгээрийн цахим орчинд ажиллах ур чадварыг зөвөөр ашиглах, хаана ажиллах боломжтой талаар зөвлөгөө мэдээлэл өгөх зорилгоор тэдэнтэй болон эцэг эхтэй нь уулзаж ярилцах, гэмт хэргээс холдуулах шат дараатай арга хэмжээг авах Цахим сонголт (CyberChoices) аяныг зохион байгуулдаг байна.

[485] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime
[486] https://www.ncsc.gov.uk/
[487] https://www.getsafeonline.org/

IV. Хууль эрх зүйн орчин

Компьютерийн зүй бус хэрэглээний тухай хууль (Computer Misuse Act 1990)[488], **Харилцаа холбооны тухай хууль** (Communications Act 2003)[489], **Хор нөлөөтэй харилцаа холбооны тухай хууль** (Malicious Communications Act 1988)[490], **Дижитал Эдийн засгийн тухай хууль** (Digital Economy Act 2017)[491], **Айлган сүрдүүлэхээс хамгаалах тухай хууль** (Protection from Harassment Act 1997)[492], **Гэмт хэрэгтэнд хариуцлага тооцох ба нийтийн хэв журмыг сахиулах тухай хууль** (Criminal Justice and Public Order Act 1994)[493] болон холбогдох бусад хууль тогтоомжоор зохицуулж байна.

Хэн нэгний нийгмийн сүлжээ болон цахим шуудангийн хаягны нууц үгийг хулгайлан дээрэлхэх, доромжлох гэмт хэрэг үйлдсэн тохиолдолд **Компьютерийн зүй бус хэрэглээний тухай** хуулиар шийдвэрлэнэ.

Бүдүүлгээр доромжилсон, зохисгүй, садар самуун болон сүрдүүлсэн, заналхийлсэн цахим зурвас илгээх нь **Харилцаа холбооны тухай** хуулийн 127-р хэсэгт заасны дагуу гэмт хэрэгт тооцогдоно.

Аливаа холбоо, харилцааны хэрэгсэл ашиглан хүнийг айлган сүрдүүлж, айдас түгшүүрт автуулах, сэтгэл санааны гутралд оруулах гэмт хэрэг үйлдсэн тохиолдолд **Хор нөлөөтэй харилцаа холбооны тухай** хуулиар шийдвэрлэдэг байна.

Дижитал Эдийн засгийн тухай хууль (Digital Economy Act 2017)-ийн 103-р хэсэгт зааснаар засгийн газар нь нийгмийн сүлжээний үйлчилгээ үзүүлэгчдэд зориулж, нийгмийн сүлжээгээр зүй бус, гэмт хэргийн шинжтэй дээрэлхсэн, доромжилсон, айлган сүрдүүлсэн утга агуулга бүхий материалыг нийтлэх, түгээхийг хориглох, холбогдох байгууллагад мэдэгдэх тухай гарын авлага боловсруулан, хэрэгжүүлж ажиллахыг хуульчилсан байна.

Мөшгих (stalking) болон цахимаар мөшгих (cyberstalking) хэргийг **Айлган сүрдүүлэхээс хамгаалах тухай** хуулийн 2А хэсгээр зохицуулна. Энэ хуулиар мөшгих гэмт хэргийн хохирогчийг хамгаалахаар заасан хэдий ч цахим халдлагын хохирогчийг давхар хамгаалдаг байна.

Тус хуулиар мөшгинө гэдэгт хэн нэгнээс салахгүй, байнгын хойноос нь даган, айдаст автуулах үйлдлийг хэлнэ гэжээ. Тодорхой хохирогчтой байнга, тогтмол холбоо барих, холбоо барих оролдлогууд тасралтгүй хийх үйлдлийг мөшгих гэнэ. Мөшгих болон цахимаар мөшгих гэмт хэрэг нь хохирогчийг байнга айлган сүрдүүлж, сэтгэл санаа болон бие махбодын хохирол учруулдаг тул хохирлын хэмжээ болон гэмт үйлдлээс хамааран 6 сараас 5 жил хүртэл хугацаанд хорих ялаар шийтгэхээр хуульчилсан байна.

Цахим гэмт хэргийн хохирогчдын дийлэнх хэсгийг хүүхэд, өсвөр насныхан эзэлж байна. Хүүхэд нь насанд хүрсэн гэмт хэрэгтнүүдийн золиос болохоос гадна үе тэнгийн хүүхдүүдийн доромжилсон, айлган сүрдүүлсэн зүй бус үйлдлийн золиос болдог байна.

[488] https://www.legislation.gov.uk/ukpga/1990/18/contents
[489] https://www.legislation.gov.uk/ukpga/2003/21/contents
[490] https://www.legislation.gov.uk/ukpga/1988/27
[491] https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted
[492] https://www.legislation.gov.uk/ukpga/1997/40/contents
[493] https://www.legislation.gov.uk/ukpga/1994/33/contents

Боловсрол болон хяналт шалгалтын тухай хуулиар сургуулийн удирдлагад сургууль, сургалтын байгууллагын эргэн тойронд суралцагч хүүхдүүд болон багш сурган хүмүүжүүлэгчдэд эрүүл, аюулгүй орчин бүрдүүлж ажиллахыг үүрэг болгосон байна. Түүнчлэн энэ хуулиар бусад сурагчдыг дээрэлхэх, доромжлох, айлган сүрдүүлэх үйлдэл байнга үзүүлж буй сурагчдыг хүмүүжүүлэх, сахилга бат сахиулах тодорхой эрхийг (тухайлбал, үүрэн телефоны утсыг хураан авах зэрэг) багш, сурган хүмүүжүүлэгчдэд олгосон бөгөөд хүчирхийлэл үйлдэгч хүүхдүүд болон тэдгээрийн эцэг, эхчүүдэд хүчирхийлэл нь тэвчиж болшгүй гэмт үйлдэл болохыг ойлгуулж, үүнийг таслан зогсоохын тулд удаа дараа хүчирхийлэл үйлдэгч хүүхдийн эцэг, эхийг шүүхийн шийдвэрээр хүүхдээ хүмүүжүүлэх албадан сургалтанд хамруулах, цаашлаад 1000 хүртэлх фунт стерлингийн торгууль ногдуулах хүртэл арга хэмжээ авахаар хуульчилсан байна.

Хүүхдийг цахимаар садар самуунд уруу татах, хулгайлах, хүчирхийлэх, бэлгийн мөлжлөгийн золиос болохоос урьдчилан сэргийлэх зорилгоор төрийн болон төрийн бус байгууллагууд нэгдэн үйл ажиллагаагаа явуулдаг байна. Засгийн газар, хууль сахиулагчид, эрдэм шинжилгээний байгууллагууд, аж ахуйн нэгжүүд, болон эцэг эхчүүдийн төлөөллөөс бүрдсэн ИБУИНХУ-ын **Хүүхдийн цахим орчны аюулгүй байдлыг хангах зөвлөл** (UK Council for Child Internet Safety)[494] нь хүүхэд, залуусын цахим орчны аюулгүй байдлыг хангахын төлөө үйл ажиллагаа явуулдаг байна.

Үндэсний Гэмт хэрэгтэй тэмцэх агентлагийн харьяа **Хүүхдийн мөлжлөг ба Онлайн хамгааллын төв** (Child Exploitation and Online Protection Center)[495] нь хүүхэд багачуудыг гэмт хэргийн хохирогч болохоос урьдчилан сэргийлж, эцэг, эхчүүд, багш, сурган хүмүүжүүлэгчид болон хүүхдүүдэд зориулсан гэмт хэргээс урьдчилан сэргийлэх, тэмцэх, таслан зогсоох төрөл бүрийн зөвлөгөө мэдээллийг багтаасан ThinkUKnow[496] цахим хуудсыг ажиллуулдаг.

Хүүхдэд харгис хэрцгий хандахаас урьдчилан сэргийлэх үндэсний нийгэмлэг (National Society for the Prevention of Cruelty to Children) нь хүүхдийн хүчирхийллийг таслан зогсоохын төлөө тэмцэгч, сайн дурын тэргүүлэгч байгууллага юм. Тус байгууллага нь хүчирхийлэлд өртсөн хүүхдүүдэд туслах, аюулд өртөж болзошгүй хүүхдүүдийг хамгаалах, хүчирхийлэл үйлдэгдэхээс урьдчилан сэргийлэх зэрэг үйл ажиллагааг хэрэгжүүлдэг байна. Тус байгууллага нь 1883 онд үйл ажиллагаагаа эхлүүлж байжээ.

Хүүхэд хамгаллын тухай хууль (Protection of Children Act 1978) [497] , **Бэлгийн хүчирхийлэлтэй тэмцэх тухай хууль** (Sexual Offences Act 2003)[498] болон холбогдох бусад хуулиар хүүхдийг бэлгийн мөлжлөгийн золиос болохоос урьдчилан сэргийлэх, энэ төрлийн гэмт хэргийг таслан зогсоох, гэмт хэрэгтэнд хариуцлага ногдуулах зэрэг харилцааг зохицуулдаг байна. Эдгээр хуулиудыг хэрэгжүүлэх ажлын хүрээнд засгийн газрын харьяа Боловсролын газар (Department for Education) нь “Хүүхдийн аюулгүй сурах орчныг бүрдүүлэх” удирдамжийг боловсруулан, сургалтын байгууллага болон эцэг, эхчүүдэд мөрдүүлэн ажиллаж байна.

[494] https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis
[495] https://www.ceop.police.uk/Safety-Centre/
[496] https://www.thinkuknow.co.uk/
[497] https://www.legislation.gov.uk/ukpga/1978/37
[498] https://www.legislation.gov.uk/ukpga/2003/42/contents

ХАВСРАЛТ

Хавсралт 1. Кибер аюулгүй байдлын чиглэлээр үйл ажиллагаа явуулж буй олон улсын байгууллагууд[499]

Байгууллагын нэр	Холбоос	Хамрах хүрээ
United Nations Internet Governance Forum	https://www.intgovforum.org/multilingual/	Global
United States National Cyber security and Communications Integration Center (NCCIC)	https://www.cisa.gov/about-cisa	National, Global
Messaging and Anti Abuse Working Group (MAAWG)	www.maawg.org	Global
Anti-Abuse Working Group	www.ripe.net	Global
Forum for Incident Response Security Teams (FIRST)	www.firest.org	Global
Asia Pacific Computer Emergency Response Team (AP CERT)	www.apcert.org	Regional
Network Operators Groups (NOGs)	https://en.wikipedia.org/wiki/Internet_network_operators%27_group	Global
Asia Pacific Economic Cooperation (APEC)	www.apec.org	Regional
ICANN Security and Stability Working Group	www.icann.org	Global
Cooperative Cyber Defense and Center of Excellence (CCDCOE)	www.ccdcoe.org	Regional, Global
Council of Europe; Convention on Cybercrime	www.conventions.coe.int	Global
INTERPOL	Interpolnyc.com	Global
Internet Society (ISOC)	www.internetsociety.org	Global

[499] https://www.itic.org/dotAsset/c/c/cc91d83a-e8a9-40ac-8d75-0f544ba41a71.pdf

Хавсралт 2. Будапештийн конвенцод нэгдэн орсон орнууд[500]

(2020 оны 6 сарын байдлаар)

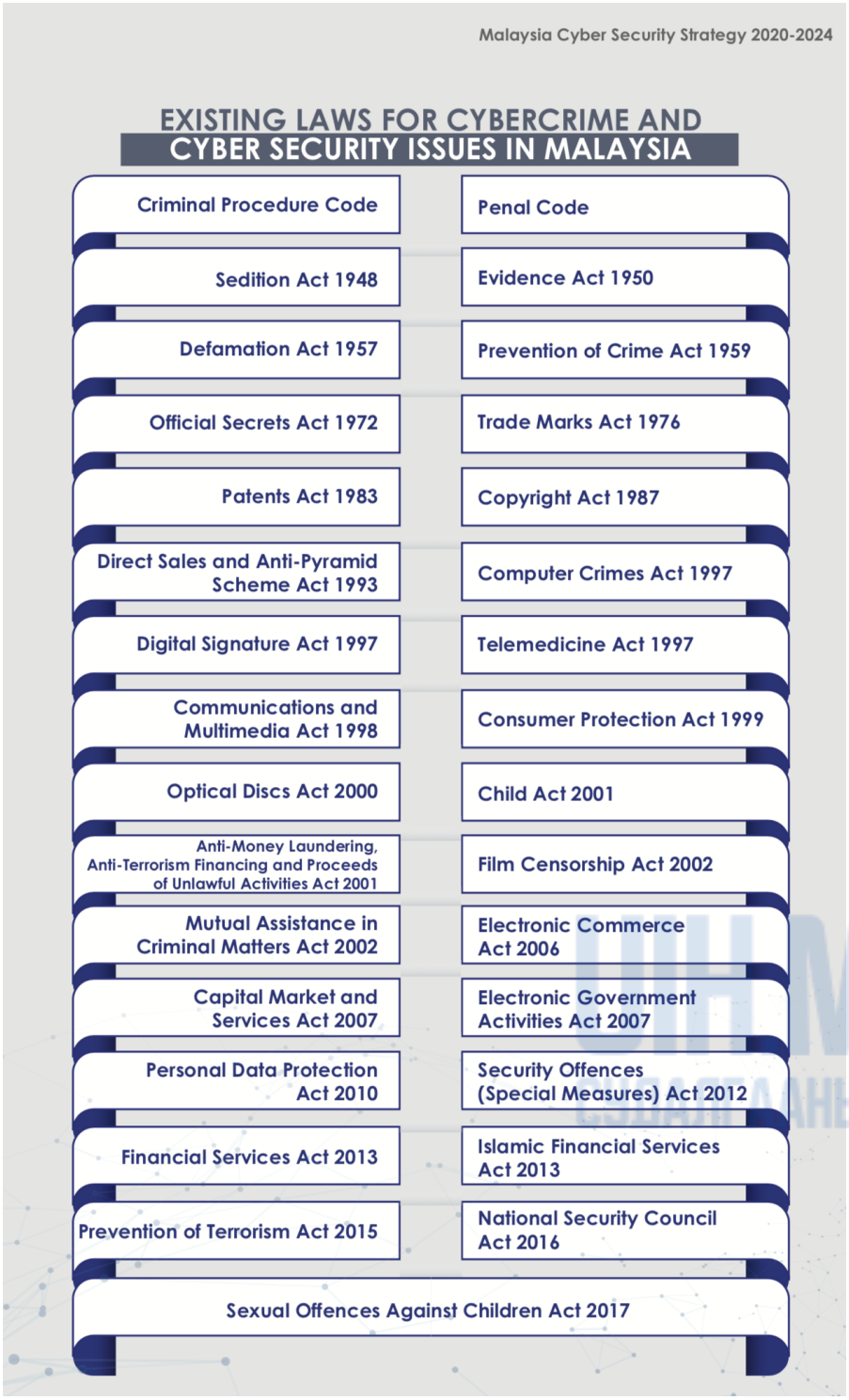
Конвенцод нэгдэн орсон улсууд	
Andorra	Latvia
Argentina	Liechtenstein
Armenia	Lithuania
Australia	Luxembourg
Austria	Malta
Azerbaijan	Mauritius
Belgium	Republic of Moldova
Bosnia and Herzegovina	Monaco
Bulgaria	Montenegro
Cabo Verde	Morocco
Canada	Netherlands
Chile	North Macedonia
Colombia	Norway
Costa Rica	Panama
Croatia	Paraguay
Cyprus	Peru
Czech Republic	Philippines
Denmark	Poland
Dominican Republic	Portugal
Estonia	Romania
Finland	San Marino
France	Senegal
Georgia	Serbia Slovak
Germany	Republic Slovenia
Ghana	Spain
Greece	Sri Lanka
Hungary	Switzerland
Iceland	Tonga
Israel	Turkey
Italy	Ukraine
Japan	United Kingdom
	United States of America

[500] https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac#:~:text=The%20Budapest%20Convention%20requires%20States,cybercrime%20but%20any%20offence%20where

Хавсралт 3. Будапештийн Кибер гэмт хэрэгтэй тэмцэх тухай конвенцын бүтэц

Бие даасан хууль	Нотлох баримт, мөрдөн байцаахтай холбоотой процедурын хууль	Олон улсын хамтын ажиллагаа
Art. 2 – Illegal access Art. 3 – Illegal interception Art. 4 – Data interference Art. 5 – System interference Art. 6 – Misuse of devices Art. 7 – Computer-related forgery Art. 8 – Computer-related fraud Art. 9 – Child pornography Art. 10 – IPR offences Art. 11 – Attempt, aiding, abetting Art. 12 – Corporate liability	Art. 14 – Scope of procedural provisions Art. 15 – Conditions and safeguards Art. 16 – Expedited preservation Art. 17 – Expedited preservation and partial disclosure of traffic data Art. 18 – Production order Art. 19 – Search and seizure Art. 20 – Real-time collection traffic data Art. 21 – Interception of content data	Art. 23 – General principles Art. 24 – Extradition Art. 25 – General rules Art. 26 – Spontaneous information Art. 27 – MLA in absence of treaty Art. 28 – Confidentiality Art. 29 – Expedited preservation Art. 30 – Partial disclosure traffic data Art. 31 – MLA accessing data Art. 32 – Transborder access Art. 33 – MLA collection traffic data Art. 34 – MLA interception content Art. 35 – 24/7 point of contact

Хавсралт 4. Малайз Улсын кибер гэмт хэрэг, кибер аюулгүй байдлын холбогдох хуулиуд



АШИГЛАСАН МАТЕРИАЛ

- Мэдээллийн аюулгүй байдлын газар http://www.isd.gov.mn/?lang=mn&cat=7
- Төрийн мэдээлэл холбооны газар https://www.cita.gov.mn/
- Эрх зүй мэдээллийн систем https://www.legalinfo.mn/
- https://www.nato.int/cps/en/natohq/topics_140739.htm
- https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf
- https://www.vmware.com/topics/glossary/content/cyber-espionage
- https://www.iso.org/standard/44375.html
- https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
- https://www.secureworldexpo.com/industry-news/countries-dedicated-to-cybersecurity
- https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/
- https://www.cyberdb.co
- https://cyberdb1.wpengine.com/database/usa/
- https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/
- https://cyberdb1.wpengine.com/database/israel/
- https://www.broadcom.com/products/cyber-security
- BSA International Cybersecurity Policy Framwork 2018 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
- https://statesassembly.gov.je/scrutinyreviewresearches/2018/research%20-%20briefing%20paper%20on%20council%20of%20europe%20convention%20on%20cybercrime%20-%2031%20october%202018.pdf
- https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac#:~:text=The%20Budapest%20Convention%20requires%20States,cybercrime%20but%20any%20offence%20where
- National center of Incidient readiness and Strategy For Cybersecutity https://www.nisc.go.jp/eng/index.html
- Japan Cybercrime Control Center https://www.jc3.or.jp/english/
- @Police https://www.npa.go.jp/cyberpolice/english/index.html
- Cybersecurity Research Institute https://www.nict.go.jp/en/csri/
- Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children https://antislaverylaw.ac.uk/wp-content/uploads/2019/08/Japan-Child-Prostitution-and-Child-Pornography-Law.pdf
- Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People https://www8.cao.go.jp/youth/youth-harm/law/pdf/for_english.pdf
- Japan Penal Code http://www.isc.meiji.ac.jp/~sumwel_h/Codes/comp-crim.htm
- Act on Prohibition of Unauthorized Computer Access http://www.japaneselawtranslation.go.jp/law/detail_main?re=01&vm=02&id=2250
- The Basic Act on Cybersecurity http://www.japaneselawtranslation.go.jp/law/detail/?printID=&re=02&vm=02&id=2760&lvm=01
- Children on the Internet https://www.jugendschutz.net/fileadmin/download/pdf/Report_2019_Children_on_the_Internet.pdf
- European Cybersecurity Month 2021 https://www.nixu.com/
- CyberSecurity Strategy for Germany 202 https://www.bundesregierung.de/breg-en/news/new-cyber-security-strategy-1958688
- Bundeskriminalamt https://www.bka.de/EN/Home/home_node.html
- Federal Ministry for Family Affairs https://www.bmfsfj.de/bmfsfj/meta/en
- BPJM https://www.bzkj.de/bzkj/meta/en

- The Commission for the Protection of Minors in the Media https://www.kjm-online.de/en/
- The Commission for the Protection of Minors in the Media https://www.kjm-online.de/en/
- Nummer gegen Kummer https://www.nummergegenkummer.de/
- Jugendschutz.net https://www.jugendschutz.net/en/index.html https://www.jugendschutz.net/en/index.html
- The Federal Review Board for Media Harmful to Minors https://www.bzkj.de/bzkj/Service/english.html
- German Law Archive https://germanlawarchive.iuscomp.org/?p=724
- Interstate Treaty on the Protection of minors https://www.kjm-online.de/
- Criminal Code (Strafgesetzbuch, StGB) https://germanlawarchive.iuscomp.org/?p=752
- Үзэл бодлоо чөлөөтэй илэрхийлэх зааг хязгаар. Фрейдрих Эбертийн сан. 2018 он.
- http://library.fes.de/pdf-files/bueros/mongolei/14077.pdf
- Network Enforcement Act https://germanlawarchive.iuscomp.org/?p=1245
- President Biden’s Executive Order https://www.mondaq.com/unitedstates/security/1074554/what39s-in-president-biden39s-executive-order-on-improving-the-nation39s-cybersecurity
- https://www.everycrsreport.com/reports/97-1025.html#:~:text=The%20Computer%20Fraud%20and%20Abuse,computers%20connected%20to%20the%20Internet.
- Prosecuting Computer Crimes https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf
- United States Code http://uscode.house.gov/search.xhtml?edition=prelim&searchString=cybercrime&pageNumber=1&itemsPerPage=100&sortField=CODE_ORDER&action=search&q=Y3liZXJjcmltZQ%3D%3D%7C%3A%3A%3A%3A%3A%3A%3A%3Afalse%3A%7C%3A%3A%3A%3A%3A%3A%3A%3Afalse%3A%7Cfalse%7C%5B%3A%3A%3A%3A%3A%3A%3A%3Afalse%3A%5D%7C%5B%3A%5D
- Cybersecurity laws and Regulations https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa
- Cybersecurity bills https://www.csoonline.com/article/3626908/18-new-cybersecurity-bills-introduced-as-us-congressional-interest-heats-up.html