



ТЕРРОРИЗМТОЙ ТЭМЦЭХ ЗӨВЛӨЛ



## ТЕРРОРИСТ ЭТГЭЭДҮҮДИЙН ЦАХИМ ОРЧИН ДАХЬ ХАРИЛЦАА ХОЛБООНЫ ТАЛААР

---

ТТЗ-ИЙН ДҮН ШИНЖИЛГЭЭНИЙ ТАНИЛЦУУЛГА  
2020-4



## ТЕРРОРИСТ ЭТГЭЭДҮҮДИЙН ЦАХИМ ОРЧИН ДАХЬ ХАРИЛЦАА ХОЛБООНЫ ТАЛААР

Европын Холбооны гишүүн орнуудын тусгай албадын зүгээс харилцаа холбооны онлайн платформ болох мессенжерийн үйлчилгээ үзүүлэгч компаниудтай хамтран террорист байгууллага, этгээдийн хооронд ашигладаг харилцаа холбооны арга замыг илрүүлэх зорилгоор хэрэгжүүлж буй арга хэмжээний үр дүнд тэдгээрийн ашиглаж байсан Telegram, Viber, Facebook, Twitter зэрэг олон төрлийн цахим платформ<sup>1</sup> дахь мессенжер бүлгэмүүдийг хаах, хязгаарлах арга хэмжээ авсаар байна. Хэдий тийм боловч террорист байгууллага, этгээдүүдийн зүгээс харилцаа холбооны шинэ платформуудыг эрэлхийлж үйл ажиллагаандаа нэвтрүүлэх, мэдээ мэдээлэл солилцох, суртал ухуулгын зорилгоор ашиглах, халдлага үйлдэх талаар мэдээлэл тараах ажлыг идэвхтэй гүйцэтгэж байна. Энэ төрлийн платформууд дээр аль болох бага мэдээлэл үлдээх, нууцлал, аюулгүй байдлыг хангах зорилгоор харилцаа холбоондоо шинэ төрлийн мессенжер аппликейшныг туршилтаар ашиглахыг эрмэлзэх болов. Ингэхдээ тухайн аппликейшнд групп чат болон тусгай суваг үүсгэх, мэдээ мэдээлэл солилцох боломж бий эсэхийг харгалзан олон нийтийн дунд түгээмэл хэрэглэгддэггүй, бизнес хөгжүүлэгч, тоглоом сонирхогч зэрэг зорилтот бүлэг рүү чиглэсэн мессенжер аппликейшн, платформуыг сонгон ашиглах нь ихсэж байна. Түүнчлэн террорист этгээдүүдийн зүгээс шинээр хэрэглэж буй платформ, мессенжер аппликейшнүүдийг хэрхэн ашиглах тухай заавар, гарын авлагыг өөрсдийн мэдээллийн сувгуудаар тараах нь элбэг болов.

Террорист этгээдүүдийн хэрэглэж буй олон нийтийн сүлжээ, аппликейшн нь дараах 3 нийтлэг шинжийг агуулдаг:

1. **User-friendliness** буюу хэрэглэхэд хялбар, өртөг бага, олон хэл дээр ашиглах, их хэмжээний дата мэдээлэл солилцох боломжтой байх;
2. **Security** буюу тухайн мессенжер аппликейшний байршиж буй сервер, эх кодыг хүн бүр харж болох эсэх, тухайн программд ямар нэгэн нууц функц бий эсэх, түүнийг ашиглах боломжтой эсэх, эдгээрээр дамжин харилцаа холбоог илрүүлэх, олзлох эрсдэлтэй эсэхийг харгалзах;
3. **Experience** буюу тухайн платформ, аппликейшнийг хэр олон хүн ашиглаж байгаа, үйл ажиллагаа нь бусдад танигдсан эсэх зэргийг тус тус харгалзан сонголт хийж байгаа аж.

*Террорист этгээдүүдийн зүгээс өөр хоорондоо мэдээлэл солилцохдоо дараах 2 төрлийн платформуыг ашиглаж байна:*






1. **DECENTRALIZED SERVER STRUCTURE** буюу төв серверээр мэдээлэл нь дамждаггүй буюу хэрэглэгчээс хэрэглэгчийн гарт шууд мэдээлэл нь илгээгддэг мессенжер үйлчилгээ юм. Ийм төрлийн үйлчилгээ ашиглаж буй террорист этгээдүүдийн хэрэглээг хянахад хүндрэлтэй байгаа учир энэ төрлийн мессенжер үйлчилгээг суртал ухуулга тараах гол сувгаа болгон ашиглах хандлагатай байгаа ба дараах аппликейшнүүдийг ихэвчлэн ашиглаж байна:

- **ROCKET.CHAT**: Бизнес эрхлэгчдэд зориулсан дуу, дүрст дуудлага, мэдээлэл солилцохдоо шифрлэх боломжтой үнэгүй аппликейшн. Windows, Linux, Mac, iOS, Android зэрэг үйлдлийн систем дээр ажиллах боломжтой ба ойролцоогоор 10 орчим сая хэрэглэгчтэй хэмээн үздэг. Хувьдаа сервер үүсгэн ашиглаж байгаа тохиолдолд хэрэглэгчийн




<sup>1</sup> Цахим платформ – Интернет хэрэглэгчдэд цахим орчинд харилцах, мэдээлэл болон үзэл бодлоо хуваалцах боломж олгодог цахим хуудас болон программууд.

мэдээллийг гуравдагч этгээд устгах боломжгүйгээс гадна үйлчилгээнд бүртгүүлэхийн тулд зөвхөн цахим шуудангийн хаяг шаарддаг. Энэхүү аппликейшнийг ашиглан Исламын улс-ДАЕШ террорист бүлэглэл өөрийн суртал ухуулгын суваг болох “Нашир ньос”-ын мэдээллийг түгээж байсан төдийгүй 2019 оны байдлаар тус сүлжээнд ДАЕШ-тай холбоотой 700 гаруй хаяг бүртгэлтэй байсныг олж тогтоожээ. Террорист этгээдүүдэд мэдээлэл технологийн дэмжлэг үзүүлдэг хэмээн буруутгагдаад буй “АФААК” медиа групп нь тус аппликейшнийг хэрхэн суулгах, ашиглах талаар гарын авлага гарган тараасан ДАЕШ террорист бүлэглэлийн зүгээс гишүүд, дэмжигчдэдээ уг аппликейшнийг хэрэглэхийг санал болгох болсон байна.

- **JABBER:** Төв серверээр дамжуулалгүйгээр дуу болон дүрст дуудлага, мэдээлэл солилцох боломжтой аппликейшн. Хэрэглэхэд хялбар, нээлттэй протоколтой учраас хэрэглэгч нь өөрийн хувийн серверийг ажиллуулж нууцлалыг хангах, интернетэд байгаа ихэнх XMPP серверүүдийг үнэгүй ашиглаж болох давуу талтай. Харилцагчид өөр хоорондоо шифрлэсэн мэдээлэл солилцох боломжтой бөгөөд шифрлэх протокол найдвартай, тайлж уншихад хүндрэлтэй, хянах боломжгүй учир террорист этгээдүүд түлхүү ашиглах болж байна. 
- **DISCORD:** Ихэвчлэн компьютер тоглоом сонирхогчид ашигладаг энэхүү аппликейшнийг iOS, Android, Linux, PC, Mac зэрэг үйлдлийн систем дээр 14 хэлээр ашиглах боломжтой. Түүнчлэн аппликейшнийг төхөөрөмж дээр суулгахгүйгээр цахим хуудсаар дамжуулан ашиглаж болдог төдийгүй бүртгүүлэхэд зөвхөн цахим хаяг байхад хангалттай. Өнөөдрийн байдлаар 250 орчим сая хэрэглэгчтэй байгаа ба нийтийн болон хувийн сервер тохируулан олон төрлийн харилцаа, холбооны суваг үүсгэж дуу, дүрст дуудлага хийх, мэдээлэл солилцох боломжтой юм. Тус аппликейшнд сөрөг мэдээллийг шүүж, устгах функц нэмэгдсэн нь террорист этгээдүүдийн зүгээс уг программыг суртал ухуулгын хэрэгсэл болгон ашиглахаас хязгаарлаж буй хэдий ч террорист этгээдүүд ашигласаар байна. 
- **RIOT.IM, MASTODON, ZERONET зэрэг бусад аппликейшн:** Дуу болон дүрст дуудлага, дата мэдээлэл солилцох хүчин чадал бүхий, олон төрлийн үйлдлийн систем дээр ашиглаж болдог үнэгүй програмууд. Олон хэлний сонголттойгоос гадна хувийн болон групп чат, тусгай нууцлал бүхий суваг үүсгэх боломжтой зэрэг онцлогтой. Террорист бүлэглэлүүд “Нашир ньос”, “Ас-сахаб” зэрэг суртал ухуулгын сувгуудын мэдээллийг байршуулж түгээдэг хэмээн тусгай албадын зүгээс үзэж байна. Зарим аппликейшн нь террорист этгээдүүдэд VPN, Tor /өөрийн мэдээллийг ил болгоогүй холболт үүсгэж болох программ/ ашиглан хувийн мэдээллээ нууцлах нэмэлт боломжийг олгодог давуу талтай.   
  


**2.CENTRALIZED SERVER STRUCTURE** буюу төв серверээр мэдээлэл нь дамжиж хэрэглэгчдэд хүрэх зохион байгуулалттай мессенжерийн үйлчилгээ. Программ хөгжүүлэгчдийн хувьд терроризмтой холбоотой мэдээ, мэдээлэл, сувгуудыг шүүж, устгах арга хэмжээ авч байгаа учир эдгээрийг ашиглах хэрэглээ цаашид ихээр нэмэгдэхгүй байх төлөвтэй байгаа ч “Нашир ньос эженси” зэрэг мэдээллийн сувгууд анхаарал татахааргүй нэр ашиглан үйл ажиллагаагаа идэвхтэй явуулж, суртал ухуулга хийж байна. Энэ төрлийн мессенжер үйлчилгээнүүдээс дараах аппликейшнуудыг идэвхтэй ашиглана:

- **HOOP** /Канад Улсын мессенжер аппликейшн/: Дуу, дүрст дуудлага хийх, мэдээлэл солилцох боломжтой, 15 хэлний сонголттой бөгөөд Android болон iOS системийг дэмждэг. Тус аппликейшн нь одоогоор 

200 мянга орчим хэрэглэгчтэй бөгөөд хувийн болон групп чатны мэдээллийг шифрлэж /end-to-encrypt/ мэдээлэл солилцох боломжийг олгодгоос гадна нууц үг ашиглан шифрлэгдсэн мэдээллийг тайлах, VAULT цэс, VPN буюу хувийн виртуал сүлжээ үүсгэх зэргээр хамгаалалт хийдэг онцлогтой юм. Террорист этгээдүүдийн зүгээс тус аппликейшнийг хувийн чат болгон ашиглахаас гадна Исламын улс-ДАЕШ террорист бүлэглэлийн суртал ухуулга явуулдаг “Нашир Ньюс” мэдээллийн сувгийг байршуулах, мэдээллийг тогтмол шинэчлэх замаар идэвхтэй үйл ажиллагаа явуулж байгаа аж. Европол буюу Европын хууль сахиулах байгууллагуудын агентлагийн мэдээлж буйгаар энэхүү аппликейшн нь террорист этгээдүүдийн ашиглаж байсан “Telegram”<sup>2</sup>-ийг орлож магадгүй хэмээн үзэж байна.

- **ТАМТАМ:** 17 хэл дээр үнэгүй ашиглах боломжтой, оросуудын зохион бүтээсэн аппликейшн бөгөөд бүхий л томоохон үйлдлийн систем дээр ажиллах, 20000 хүртэл гишүүнтэй групп үүсгэх нэмэх боломжтой. Исламын улс-ДАЕШ террорист бүлэглэлийн зүгээс энэхүү аппликейшнийг ашиглах нь нэмэгдэж байгаа хэдий ч ТАМТАМ-ын хөгжүүлэгчдийн зүгээс терроризмтой холбоотой хаяг, группыг тогтмол хааж байгаа талаар мэдэгдэж буй.
- **THREEMA:** 3 еврогийн төлбөртэй, 11 хэл дээр ашиглах боломжтой тус аппликейшнийг ашиглах зааврыг AFAAQ медиа группээс гаргасан бөгөөд нууцлал, аюулгүй байдал сайн хангагдсан хэмээн үзэж террорист этгээдүүдийн дунд түгээмэл тархаж байгаа аж.



**ДҮГНЭЛТ:** Террорист этгээдүүдийн харилцаа холбооны гол хэрэгсэл “Telegram” дахь сувгуудыг хаасны дараагаар ямар платформ суртал ухуулгын гол хэрэглээ болох нь бүрэн тодорхойгүй байгаа бөгөөд террорист этгээд нь үйл ажиллагаагаа тогтмол үргэлжлүүлэхийн тулд дээрх мессенжер үйлчилгээнүүдийг өргөнөөр ашиглах төлөвтэй байна. Тэд өөрсдийн таних тэмдэг, лого, нэр зэргийг ашиглахаас зайлсхийж байгаа нь тэдний групп болон сувгийг илрүүлэх, устгахад хүндрэлтэй байгаа ч цаашид уг хүндрэлийг шийдвэрлэх боломжтой хэмээн тусгай албадын зүгээс үзжээ.

Хандалт ихтэй томоохон цахим платформууд аюулгүй байдлаа бэхжүүлэх арга хэмжээг тухай бүр авч байгаа нь террорист этгээдүүд тус платформуудыг өдөр тутмын үйл ажиллагаандаа ашиглах боломжийг хязгаарлаж байна. Нөгөөтэйгүүр бизнес хөгжүүлэгч, тоглоом сонирхогч зэрэг зорилтот бүлэг иргэдэд тусгайлан зориулсан жижиг цахим платформуудыг террорист этгээдүүд үндсэн зориулалтаар нь бус буюу өөрсдийн хэрэгцээндээ тохируулан ашиглах тохиолдол нэмэгдсээр байна. Нэгэнт мессенжер, олон нийтийн сүлжээ, серверийг шинээр бий болгож, хөгжүүлэн олон нийтэд түгээх нь нээлттэй учир террорист этгээдүүдэд боломж үргэлж байх хэдий ч гагцхүү тухайн харилцаа холбооны сүлжээг тодорхойлж, хяналтдаа байлган холбогдох арга хэмжээг тухай бүр авч байх нь террорист үйл ажиллагаанаас урьдчилан сэргийлэх, таслан зогсоох боломжийг олгоно.

## ТЕРРОРИЗМТОЙ ТЭМЦЭХ ЗӨВЛӨЛИЙН АЖЛЫН АЛБА

### АШИГЛАСАН МАТЕРИАЛ:

1. A growing frontier for terrorist groups: Unsuspecting chat apps (wired.com, September 2019)
2. Terrorist groups are moving to niche chat platforms (fairplanet.org, March 2019)

<sup>2</sup> Telegram – Террорист байгууллага, этгээдүүд өргөнөөр ашиглаж байсан 200 сая гаруй идэвхтэй хэрэглэгчтэй ОХУ-ын мессенжерийн аппликейшн бүхий харилцаа холбооны сүлжээ.