Security Solution & Service

ӨНӨӨДРИЙН МОНГОЛ УЛС БОЛОН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДАЛ

Т.ХАЛТАР

Зөвлөх

Товчхон

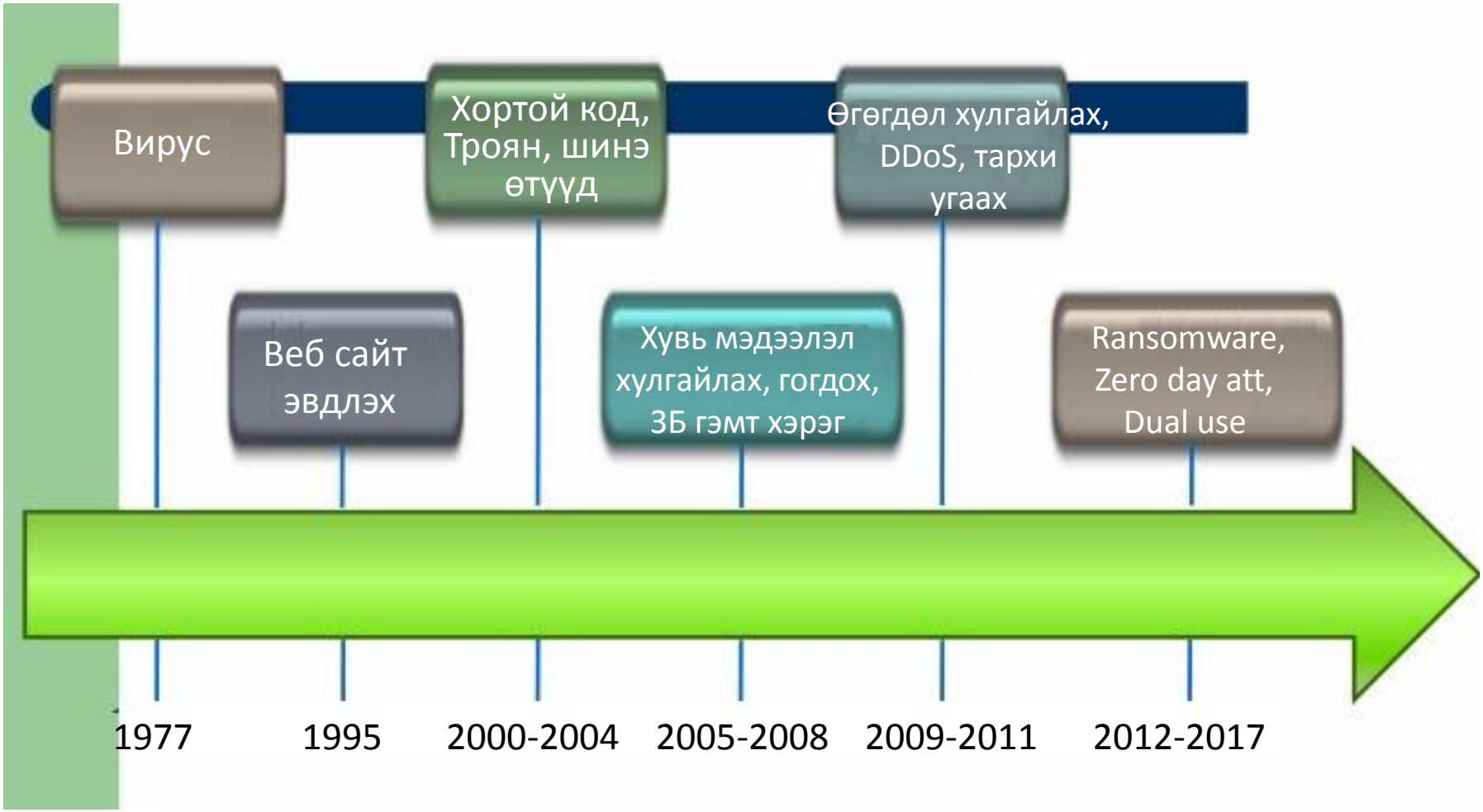
Мэдээллийн Технологийн 3 дахь эрин үеийг тодорхойлж буй 4 том хүчин зүйл бидний амьдралд асар олон боломжийг олгож байна

- **Cloud** буюу Үүлэн тооцоолол,
- **Big Data** буюу геометр прогрессоор өсөн нэмэгдэж буй үлэмж хэмжээний тоон мэдээлэл,
- **Social** буюу Нийгмийн сүлжээ,
- **Mobility** буюу хөдөлгөөнт төхөөрөмж, ухаалаг гар утасны өргөн хэрэглээ
- Хармсалтай нь сайн юманд саар дагалддаг жамаар төрөл бүрийн кибер халдлага, тагнан турших ажиллагаа, будлиан зөрчил ихэссээр

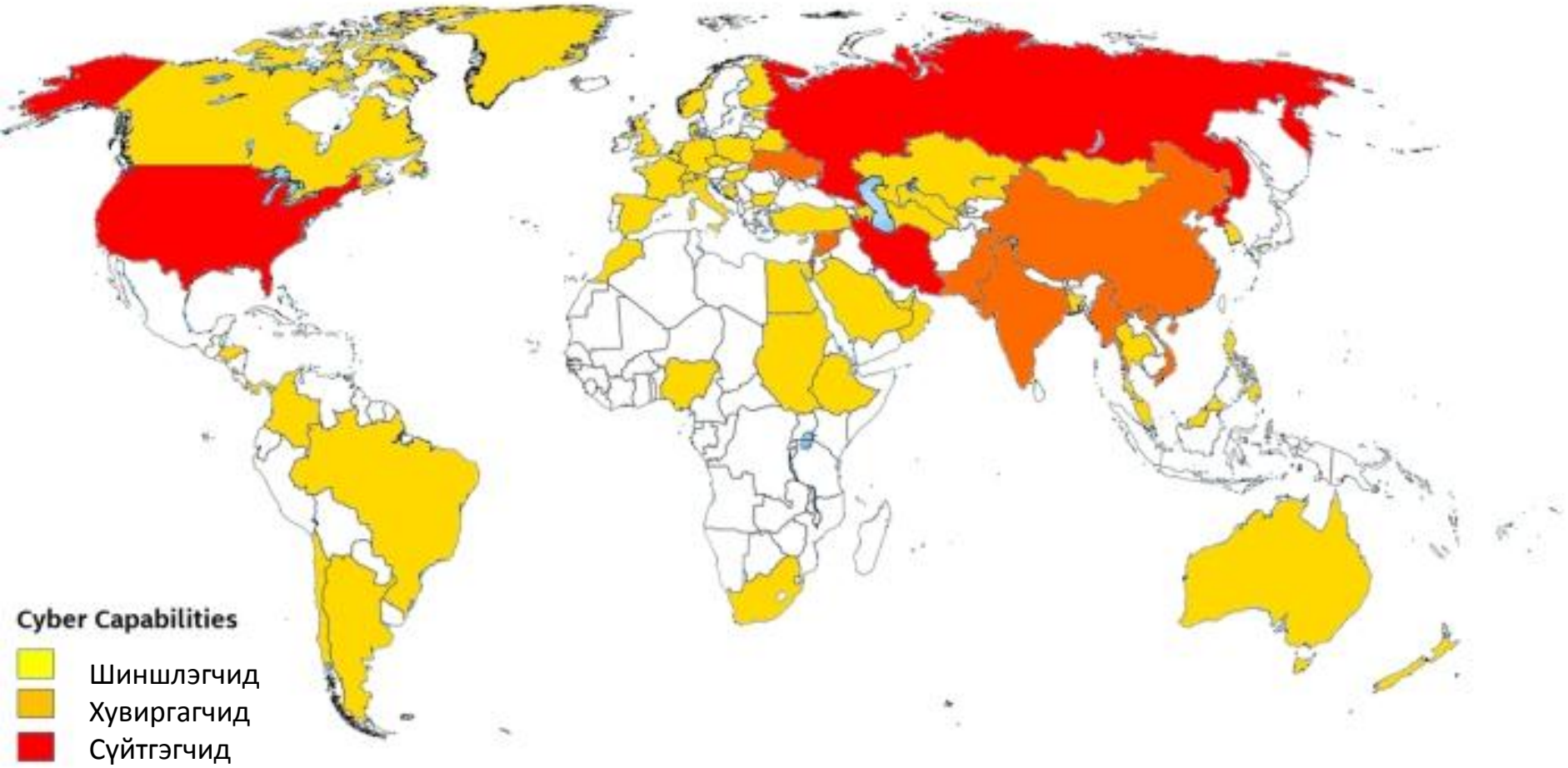
Халдлагын чиг хандлага

- 2015 онд кибер халдлагын тоо өмнөх онтой харьцуулахад 38%-аар өссөн
- нийт кибер халдлагуудын 38% нь хэдхэн секундын дотор, 60% нь хэдхэн минутын дотор компанийн мэдээллийн системд нэвтэрч, 28% нь систем дэх бүх өгөгдлийг ердөө хэдхэн минутад бүрэн хулгайлан авч байгаа
- Кибер халдлагад өртсөн байгууллагын 58% нь халдлагад өртсөнөө хэдэн долоо хоногоос хэдэн сар, улирал дамнан мэдээгүй байдаг
- Монголд ихэнх байгууллага өөрсдийн мэдээллийн бүрэн бүтэн байдал, нууцлалыг хянаж чаддаггүй, гадагш алдагдаж урсаж байгаа эсэхийг огт мэддэггүй.

Өөрчлөгдөн хувьсаж буй аюулууд



Кибер дайны төвүүд



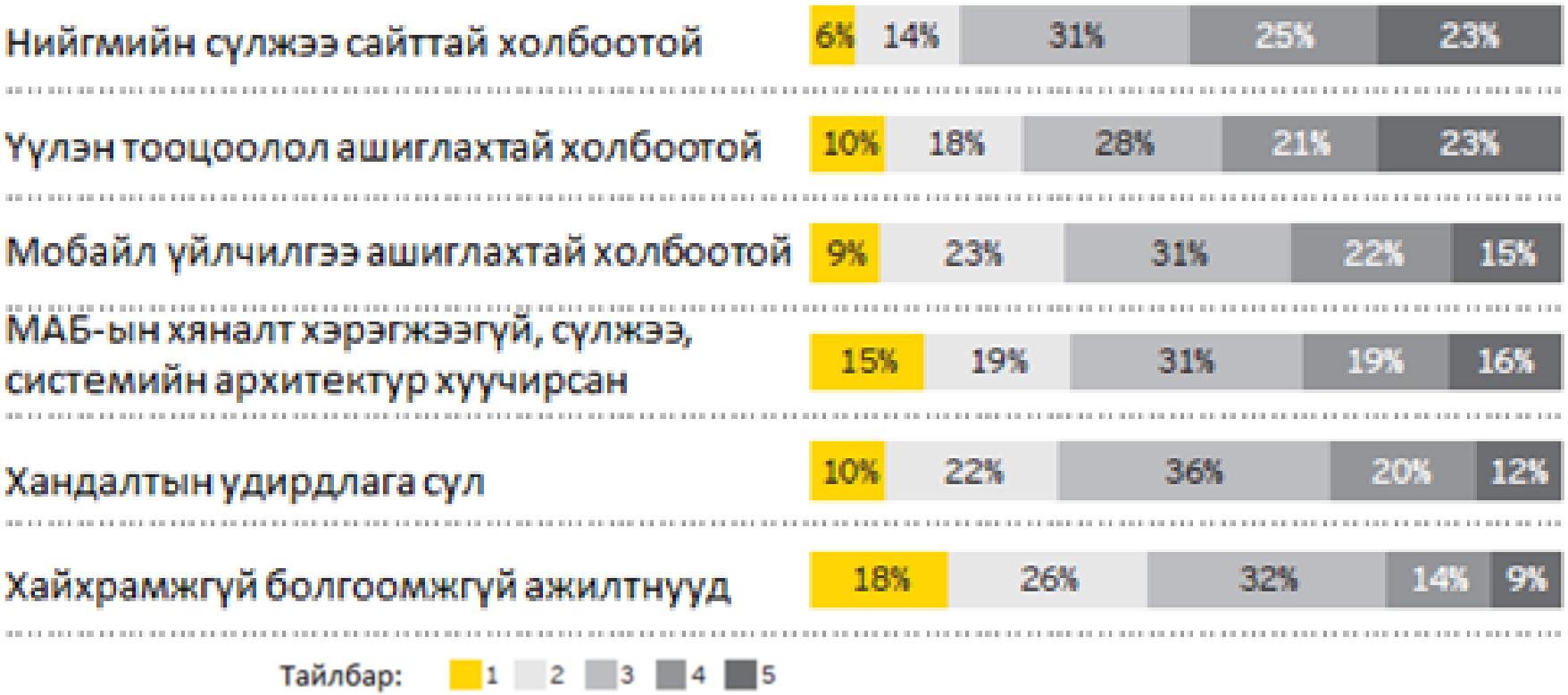
Өнөөдрийн кибер дайн

- Кибер зэвсэг, кибер арми
- Кибер тагналтын арга, технологи, техник хэрэгсэл
- Уламжлалт антивирус, интернет аюулгүй байдлыг програм хангамжууд орчин үеийн байлдааны зориулалттай хортой кодуудын эсрэг юу ч хийж чадахгүй
  - Flame, Stuxnet, DuQu, Stealthy malware
- Zero day халдлага, Ransomware хортой код, Advanced Persistent Threat (APT)

Өнөөдрийн Монгол болон кибер дайн

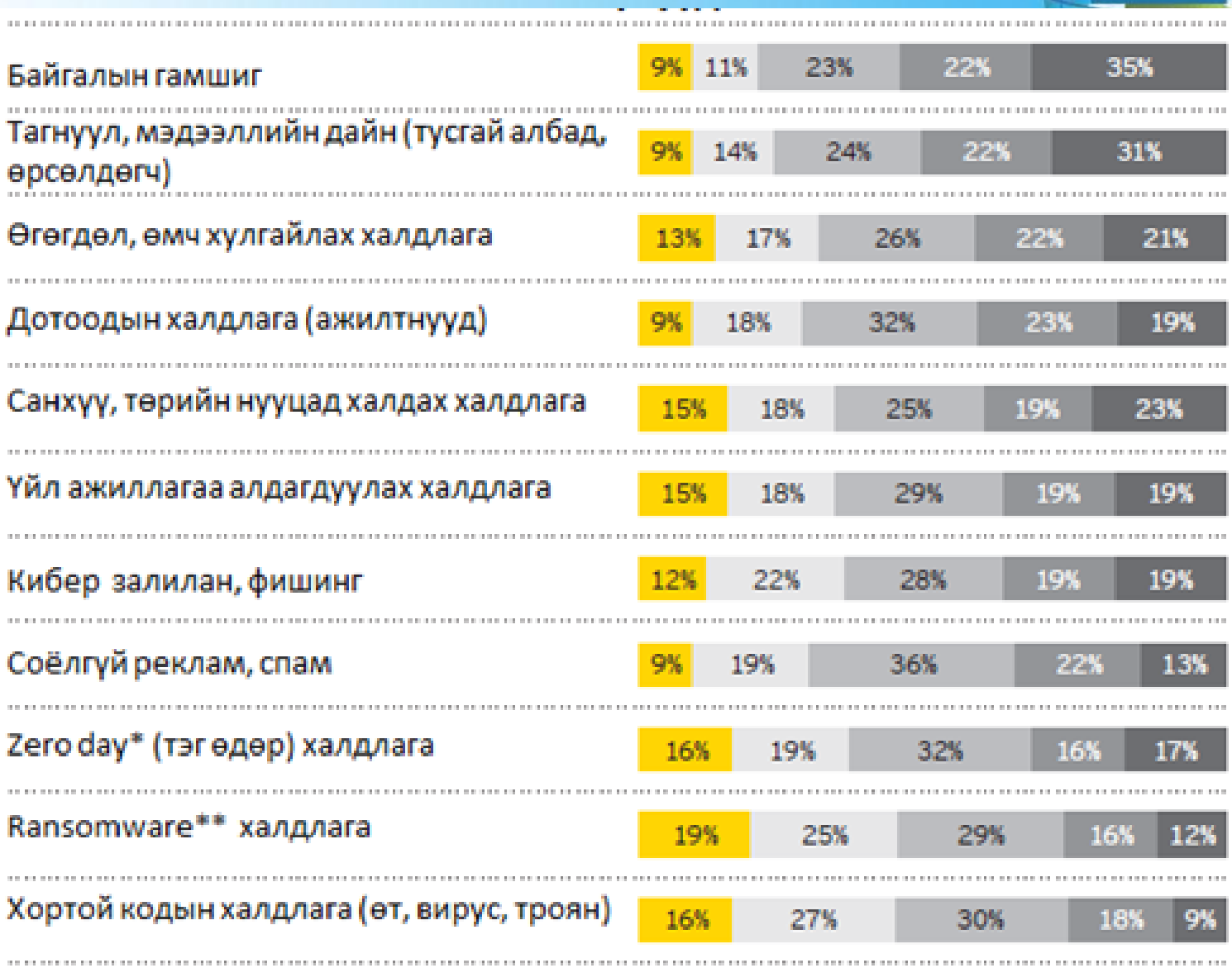
- Бүдүүлэгдүү, бяд муутай
- Бусдын өгөөш болгосон зүйлсийг шууд залгих,
- Нийгмийн сэтгэхүйгээ удирдуулах,
- Систем, сүлжээгээ ухуулах,
- Өгөгдлөө гадагш урсгаж алдах,
- Бодит мэдээллийг ашиглах биш хагас үнэн, хуурмаг мэдээллийг хэн сайн зохиож, олон нийтэд чадварлаг итгүүлснээрээ ялагч болох
- МАБ-ын эрсдэлийн шинжилгээгээ ойлгодоггүй
- Зорилго чиглэлтэй удирдлага, тогтолцоо, цогц арга хэмжээ, бодлого хэрэгжүүлж чадаагүй
- Сүлжээний нэгдмэл хяналт, мониторинг огт хийгддэггүй
- Учрал, зөрчил, будлианыг мэдээлдэг тогтолцоо, журам байхгүй
- Мэдээллийн аюулгүй байдлын аудит огт хийлгэдэггүй,
- Сүлжээ, тоног төхөөрөмжүүдийн тест туршилт огт хийж байгаагүй
- **Технологийн асар их хамааралтай**

Монголын нийтлэг эмзэг байдал



1: Маш ноцтой болсон
2: Ноцтой байна
3: Аюултай байна
4: Багагүй эрсдэл учруулж байна
5: Хүлээн зөвшөөрч болохуйц байна

Тулгарч буй нийтлэг аюул



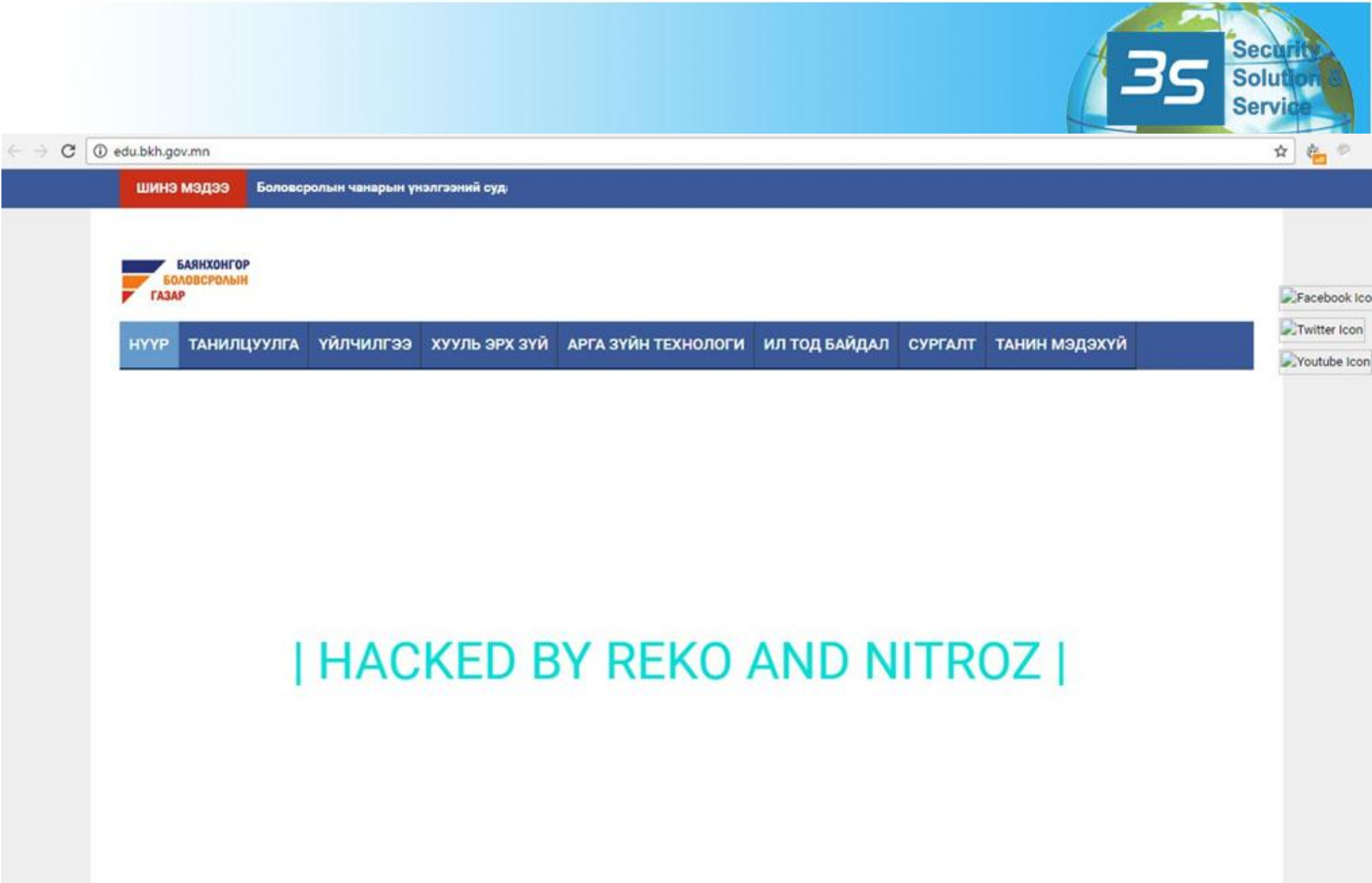
Орчин үеийн халдлагын эх сурвалж

Сүүлийн үеийн хакердуулсан веб сайтууд

Date	Notifier	H	M	R	L		Domain	OS	View
2016/12/01	ALP3R	H	M				orshilconstruction.mn	Linux	mirror
2016/11/24	Expired	H					specialmongolia.mn	Linux	mirror
2016/11/23	TurkishSpyHacker						gofundme.mn/Turk.html	Linux	mirror
2016/11/21	chinafans						victorysports.mn/x.txt	Linux	mirror
2016/11/17	CyBeRKaNKa	H	M				weblink.khunnu.mn	Linux	mirror
2016/11/16	Aris Dot ID		M				asar-maikhan.mn/x.txt	Linux	mirror
2016/11/08	CyBeRKaNKa	H	M				sumber.nemekh.mn	Linux	mirror
2016/11/08	CyBeRKaNKa	H	M				galt.nemekh.mn	Linux	mirror
2016/11/08	CyBeRKaNKa	H					nemekh.mn	Linux	mirror
2016/11/01	jok3r			R			pch4.mn/images/jdownloads/scre...	Linux	mirror
2016/10/25	jok3r	H					khanuul.procurement.gov.mn	Linux	mirror
2016/10/20	Index Php			R			zaamar.to.gov.mn/zxcvbnm.gif	Linux	mirror
2016/10/18	Spyhackerz.com	H		R			www.nta.mn	Linux	mirror
2016/10/04	./UnIX						ganabell.mn/ds.html	Linux	mirror
2016/09/30	N61tap						www.ikh-ishtolgoi.mn/p.htm	Linux	mirror
2016/09/30	N61tap						www.crusher-screen.mn/p1.txt	Linux	mirror
2016/08/30	VirtuaL	H					ces.gov.mn	Win 2008	mirror
2016/08/30	VirtuaL	H					ajil.gov.mn	Win 2008	mirror
2016/08/24	Mr.Kro0oz.305		M				lhagvadorj.mn/i.htm	Linux	mirror
2016/08/09	chinafans			R			www.chinggisbeer.mn/xx.htm	Win 2008	mirror
2016/08/01	KkK1337						jobagency.mn/job/images/other/...	Linux	mirror
2016/07/26	kevin (mr.k)						www.0479.mn/yolo.html	Win 2003	mirror
2016/06/28	jok3r			R			www.soyolerdem.edu.mn/images/f...	Linux	mirror
2016/06/28	Code Breaker		M	R			taiyobridge.mn/x.html	Linux	mirror
2016/06/28	Code Breaker			R			wsp.mn/x.html	Linux	mirror

Үргэлжлэл

Time	Notifier	H	M	R	L		Domain	OS	View
2016/10/19	Gekikara404						noah.mn/mion.php	Linux	mirror
2016/10/15	Reko					★	bnd.ub.gov.mn/?p=22375	Linux	mirror
2016/10/09	Reko	H				★	edu.bkh.gov.mn	Linux	mirror
2016/10/07	Turan Ordusu	H		R			www.alutech.mn	Linux	mirror
2016/09/20	./r0cky_n00bz	H					khiimori.mn	Linux	mirror
2016/09/01	Prosox					★	kr.immigration.gov.mn/?p=2824	Linux	mirror
2016/09/01	Prosox	H				★	police.gs.gov.mn	Linux	mirror
2016/08/25	Team System Dz	H				★	fipds.mcaa.gov.mn	Linux	mirror
2016/08/25	Team System Dz	H				★	khovd.mcaa.gov.mn	Linux	mirror
2016/08/25	Team System Dz	H				★	nubia.mcaa.gov.mn	Linux	mirror
2016/08/25	Team System Dz	H		R		★	www.mcaa.gov.mn	Linux	mirror
2016/08/25	Team System Dz	H		R		★	ans.mcaa.gov.mn	Linux	mirror
2016/08/18	Er0iN						cs.skylink.mn/sh_stats/sh_hero...	Linux	mirror
2016/08/09	moftah-deeb			R			minjzand.mn/maile/mailer.php	Linux	mirror
2016/07/24	AGroup						www.mne.mn/mn/search	Linux	mirror
2016/07/15	attacker	H		R			ardchilal.mn	Linux	mirror
2016/07/08	TuranOrdusu	H				★	bgots.ub.gov.mn	Linux	mirror
2016/07/04	Dr.Muneer	H				★	bangkok.mfa.gov.mn	Linux	mirror
2016/05/18	CyBeRKaNKa	H					eng.iieb.mn	Linux	mirror
2016/04/30	LuXas			R		★	bayangol.hudulmur.gov.mn/image...	Linux	mirror
2016/04/15	CyBeRKaNKa	H					weblink.khunnu.mn	Linux	mirror
2016/04/15	ZoRRoKiN					★	burtgel.gov.mn/tamga/stamp.rep...	Linux	mirror
2016/04/03	MR ABAN	H					www.oe.org.mn	Linux	mirror
2016/03/25	OniXeeMa	H					www.aerogeodesy.mn	Linux	mirror
2016/03/19	AHFÅ TECENNÜN						mnnf.mn/site/	Linux	mirror



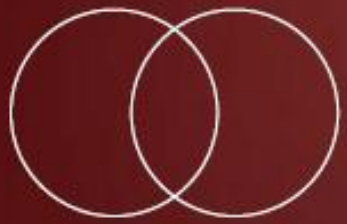
Мэдээллийн аюулгүй байдлын гурвалжин

МАБ-ыг хангах удирдлагын тогтолцоо, арга хэмжээ

Ирээдүйн хандлага

1980

1990



21-р зуун

Ижил орон зай, дундын эрсдэл

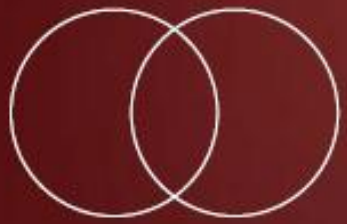
1980

ОУ-ын эдийн засаг
-өрсөлдөгчид
-Тагналт

Кибер орон зай
- хакерууд
-өгөгдлийн хулгай

1990

ОУ-ын эдийн засаг



Кибер орон зай

21-р зуун

ОУ-ын эдийн засаг
- Хакерууд
-өгөгдлийн хулгай

Кибер орон зай
-өрсөлдөгчид
-Тагналт

Шинэ эриний аюулууд

Шинэ Технологийг даган кибер аюул, эрсдлийн мөн чанар өөрчлөгдөж байна. Шинэ үе хэдийн дүрмээ шинэчилсэн – кибер аюулууд насанд хүрч одоо улам нарийн, төвөгтэй, төгс шинжрүүгээ шилжиж байна.

Таамаглал

- DoS халдлагууд 2021 онд гол довтолгоон байхаа больж том уялдуулсан халдлагын нэг хэсэг болж хувирна.
- Кибер активизм илүү өргөн хүрээтэй болж үг хэлэх эрх чөлөө болон аюулгүй байдлын тэнцвэрийн асуудал толгойн өвчин болно.
- Дэлхийн хэмжээний кибер дайн 2021 он гэхэд эхэлнэ. Энэ нь зарлаагүй дайн юмуу өөр нэртэй байх болно.
- 2021 он гэхэд кибер гэмт хэргээс учрах хохирол 5-10 их наяд долларт хүрнэ.
- Ихээхэн хүч чармайлт гаргасан ч дэлхийн кибер дэд бүтэц эмзэг хэвээр байх болно.
- Кибер хорт санаатнууд давуу байдлаа хадгалсаар үлдэнэ.

Таамаглал (үргэлжлэл)

- “Мэдээллийн баталгаа” гэдэг ойлголт “Кибер баталгаа” болж солигдоно
- IPS, галт хана, замчлагч болон бусад АБ төхөөрөмжүүд нэгдсэн бодлогын удирдлагын доор уялдаж, түүнийг дэмжинэ.
- Нийгмийн боловсруулалтын стратеги нь Кибер аюулгүй байдлын практиктай бүрэн нэгдэнэ.
- Байгууллага илүү виртуаль болж ихэнх ажлаа цахимаар нэгдэж хийнэ.
- Гэрчилгээ, баталгаажуулалт алга болж бодит цаг үед бодит горимоор хийгддэг мониторинг, баталгаажуулалтаар солигдоно.

Хамгаалалтын хандлага

- Сүүдрийн МТ-ийн эсрэг хамгаалалт
- Хандалтын нэг эрх, адилтгал
- Гуравдагч талын бүртгэлийн өгөгдөл
- Олон хүчин зүйлт хандалтын удирдлага
- Том өгөгдлийн шинжилгээ
- Олон давхаргат аюулгүй байдал
- Мобайл хамгаалалт
- Интернет эд юмсын аюулгүй байдал
- Хүн болгоны үүрэг, хариуцлага, мэдлэг, ойлголт, аюулгүй зан үйл, хэрэглээ
- Кибер түншлэл
- Аюулгүй ажлын орчин
- Мэдээллийг зохистойгоор дундаа ашиглах
- Төрийн доторх болон гадаад хамтын ажиллагаа
- Эрсдэлд суурилсан аюулгүй байдал

Анхаарал тавьсанд баярлалаа

khaltar@sssmn.com

99153286