2-дәріс. Экстремистік мәліметтер түсінігі. Экстремизм категориялары. Кибертерроризм, киберсоғыс түсініктері

Тақырыптың өзектілігі

Жаһандық желіде агрессивті ақпараттың таралуына қарсы тұру қоғам мен мемлекеттік органдардың өзекті мәселесі болып табылады, ол әсіресе интернеттің қажетсіз ресурстарын сүзу арқылы шешіледі.

XXI ғасыр технологиялары интернеттегі ақпаратты пайдалануды кеңейткенімен, мәтіндік деректер интернеттегі мазмұнның ең көп таралған түрі болып табылады. Алайда, террористік және экстремистік топтар ақпарат тарату, насихаттау, қаражат жинау, жалдау және экстремистік миссияларын қоса алғанда, әртүрлі функцияларды орындау үшін веб-технологияларды енгізуде. Мұндай жағдайда интернет ұлттық қауіпсіздікке қауіп төндіреді.

Интернет экстремистік материалдарды орналастыру үшін белсенді қолданылып келеді. Проблема жалпы әлемдік сипатқа ие және әлемдік саяси процестің басты қатысушыларының бірі ретінде Қазақстан Республикасы үшін өте өзекті. Интернеттің ғаламдық желісін және компьютерлік байланыс мүмкіндіктерін қолдана отырып, экстремистік қозғалыстар мен топтардың идеологтары азаматтардың, ең алдымен жастардың санасына белсенді әсер етеді.

Экстремистер бүгінде қылмыстық іс-әрекетте Интернет желісінің шын мәнінде шексіз мүмкіндіктерін белсенді пайдаланады, оның ішінде: қылмыстарды дайындау және жасау кезінде Интернет желісінің ресурстарын пайдалану; әлеуметтік қауіпті әрекеттерді басқару және ұйымдастыру мақсатында ақпаратпен жасырын алмасу; экстремистік қызметті қаржыландыру үшін иесіздендірілген қаржылық желілік құралдарды қолдану, мысалы Darkcoin төлем жүйелері; арнайы құрылған сайттарда және басқа интернет-ресурстарда белсенді насихаттау үшін жоспарланған ақпараттық операцияларды жүзеге асыру және т.б. нәтижесінде соңғы жылдары экстремизм проблемасы шиеленісе түсуде, ол қазіргі уақытта жалпы мемлекеттік маңызы бар проблема және Қазақстанның ұлттық қауіпсіздігіне қатер ретінде қаралуда. Осылайша, интернет желісін пайдалана отырып, экстремистік көріністерге қарсы іс-қимыл саласындағы ахуал күрделі болып қалуда, бұл, атап айтқанда, экстремизмнің кез келген көріністерін анықтауға, олардың алдын алуға және жолын кесуге бағытталған ғылыми зерттеулерді жүзеге асыру және тиімді әрі уақтылы шаралар кешенін іске асыру қажеттілігін негіздейді.

Экстремизм мәселесі ежелгі дәуірден бастап бүгінгі күнге дейін отандық және шетелдік ғылыми әдебиеттерде зерттелуде. Бүгінгі таңда экстремизм әртүрлі зерттеулердің объектісі болып табылады. Экстремизм құбылысы өте серпінді дамып, күн сайын жаңа белгілер мен сипаттамаларға ие болуда. Қазіргі уақытта үгіт-насихат пен экстремистік идеологияның әсерінен террористердің, сондай-ақ желілік және әлсіз байланысқан құрылымы бар ұйымдасқан террористік қауымдастықтардың, террористік шабуылдарының саны артып келеді.Ақпарат алмасудың, жалдаудың және осындай құрылымдарды жылжытудың негізгі құралы – интернет,атап айтқанда веб-ресурстар, әлеуметтік желілер және электрондық пошта. Осыған байланысты интернет желісінде террористік және экстремистік ақпаратты генерациялайтын және тарататын жекелеген пайдаланушылардан, топтардан және желілік қоғамдастықтардан туындайтын қатерлерді анықтау, қарым-қатынас тақырыптарын, байланыстарды айқындау, сондай-ақ мінез-құлық мониторингі және болжау міндеті туындайды.

Қазіргі уақытта экстремистік әрекетке қарсы күрес Қазақстан Республикасының аумағында да, одан тыс жерлерде де болып жатқан оқиғалармен анықталған құқық қорғау органдарының басым міндеттерінің бірі болып табылады. Дегенмен, шамамен 15-20 жыл бұрын экстремистік топтар мен қозғалыстардың қызметі қаланың, облыстың немесе ауданның кеңістіктік шекараларымен оқшауланды, ал қазір интернеттің арқасында экстремизм әлем елдерінің ақпараттық күн тәртібінде ауқымды элементке айналуда.

Экстремистік қозғалыстардың мүшелері пікірталастарға қатысуға, олардың идеологиясы мен мүдделерін әртүрлі интернет-ресурстарда қорғауға мүмкіндік алды, онда адамдар саны өте көп және бірнеше ондағаннан жүздеген мың адамға дейін жетеді. Шетелдік зерттеулерден алынған мәліметтерге сүйене отырып, интернет желісінде он мыңға жуық экстремистік электрондық көздер бар екендігін анық айтуға болады. Бұл жүйенің негізін араб тіліндегі сайттар құрайды, олардың саны шамамен екі-үш мың. Экстремистік желі интернет арқылы насихаттауды таратудың тиімді әдісін жасады. Бұл сайттарға кірушілер экстремистік сипаттағы материалдарды көшіреді, сондай - ақ оларға сілтемелер жасайды, оларды экстремистік және экстремистік емес бағыттағы басқа сайттарға таратады.

Компьютерлік әлеуметтік ғылымдар қауымдастығының зерттеушілері қоғамды түсіну үшін интернеттегі әлеуметтік желіні зерттеудің маңыздылығын көрсетті. Қазіргі жағдайда интернеттегі экстремизм көріністеріне қарсы тұру көбінесе әлеуметтік құбылысты талдаудың объективтілігі мен тереңдігіне, деструктивті күштердің мазмұнын, стратегиясы мен тактикасын одан әрі дамыту тенденцияларын болжауға байланысты болады. Ақпараттық-психологиялық әсер ету арқылы қоғамды басқару тәсілі, экстремизм идеологиясының таралу қаупі одан да қауіпті болып келеді және мемлекеттік құрылымдар тарапынан тиісті қарсы іс-қимыл шараларын қолдануды көздейді. Деструктивті күштердің қызметін уақтылы анықтауға және жолын кесуге мүмкіндік беретін құралдардың бірі интернеттің ақпараттық ресурстарына мақсатты мониторинг жүргізу болуы тиіс.

Экстремизм түсінігі

Экстремизм (фр. exremisme, лат. extremus - төтенше) - бұл қоғамдағы нормалар мен ережелерді түбегейлі жоққа шығаратын экстремалды көзқарастар мен іс-әрекеттерді ұстану. Экстремизмнің негізгі негізі – қандай да бір идеялық мазмұнмен және мағынамен толтырылған агрессивтілік. Экстремизмді әртүрлі әлеуметтік немесе мүліктік жағдайы, ұлттық және діни құрамы, кәсіби және жоғары білім деңгейі бар және т.б. бар адамдар жүзеге асыра алады. Қазіргі таңда жастардың экстремистік мінез-құлқының өзіндік ерекшелігі бар: ұлттық, діни және саяси себептермен зорлық-зомбылық жасау. Экстремизм ауқымдылығы бойынша келесідей ерекшеленеді: жеке индивидтің экстремистік көріністері; шағын топтардың (100 адамға дейін) және ірі топтардың (100 адамнан астам) экстремистік көріністері; мемлекеттер мен ұлтаралық бірлестіктердің саясатындағы экстремистік көріністер.

Экстремизм түсінігі

Экстремизмнің түрлері ортақ белгілермен сипатталады: зорлық-зомбылық немесе оның қауіп-қатері (әдетте қарулы күшпен); бір өлшемділік, әлеуметтік мәселелерді қабылдауда біржақтылық, сондай-ақ оларды шешу жолдарын іздеу; өз принциптері мен көзқарастарын қарсыластарға тануға деген ұмтылыс; кез-келген бұйрықтар мен нұсқауларды сөзсіз орындау; сезімдер мен инстинкттерге сүйену, бірақ ақылға емес; толеранттылыққа, ымыраға келуге немесе оларды толығымен елемеуге қабілетсіздік. Экстремизм шектен тыс радикализммен, терроризммен және нигилизммен ұштасады. Экстремизмнің себептері азаматтардың бір бөлігінің әлеуметтік бағдарлануында, тиісті білімнің болмауында, қоғамның дағдарыстық жағдайында, сондай-ақ құқықтық жүйенің тиімсіздігінде жатыр. Экстремизм саяси, экономикалық, әлеуметтік, діни және қоғамдық өмірдің басқа салаларында жиі кездеседі. Экстремизм – қазіргі заманның өткір мәселесі.

Экстремизм – бұл:

- адам мен азаматтың құқықтары мен еркіндігіне қол сұғу, адамдардың наным-сенімдері, нәсілдік немесе ұлттық тиістілігіне, дініне, әлеуметтік жағдайы немесе әлеуметтік шығу тегіне байланысты олардың денсаулығы мен мүлкіне зиян келтіру;
- рұқсат етілмеген баспа, аудио-аудиовизуалды және басқа да материалдарды құру және тарату;
- мемлекеттік немесе қоғамдық қызметкерге оның мемлекеттік немесе басқа да саяси қызметін тоқтату мақсатында немесе кек алу мақсатында шабуыл жасау;
- ҚР конституциялық құрамы мен тұтастылығын күштеп өзгерту;
- Терроризмді ашық түрде қолдау немесе террористік іс-әрекетті орындау;
- Әлеуметтік, нәсілдік, ұлттық немесе діни дауды тудыру;
- Саяси, идеологиялық, нәсілдік, ұлттық немесе діни жеккөрушілік немесе қандай да бір әлеуметтік топқа қарсылассу мотивтері бойынша қылмыс жасау;

- адамның әлеуметтік, нәсілдік, ұлттық, діни немесе тілдік қатыстылығы немесе дінге көзқарасы негізінде оның айрықшалығын, артықшылығын немесе кемтарлығын насихаттау;
- азаматтардың өздерінің сайлау құқықтарын және референдумға қатысу құқықтарын жүзеге асыруына кедергі келтіру немесе зорлық-зомбылықпен не оны қолдану қатерімен ұштасқан дауыс беру құпиясын бұзу;
- мемлекеттік органдардың, жергілікті өзін-өзі басқару органдарының, сайлау комиссияларының, қоғамдық және діни бірлестіктердің немесе өзге де ұйымдардың зорлық-зомбылықпен не оны қолдану қатерімен ұштасқан заңды қызметіне кедергі жасау;
- нацистік атрибутиканы немесе символизмді, нацистік атрибутикаға немесе символизмге ұқсас атрибутиканы немесе символизмді араластыру деңгейіне дейін насихаттау және көпшілікке көрсету немесе экстремистік ұйымдардың атрибуттарын немесе символикасын көпшілікке көрсету;

- көрсетілген іс-әрекеттерді жүзеге асыруға жария түрде шақыру не көрінеу экстремистік материалдарды жаппай тарату, сол сияқты оларды жаппай тарату мақсатында дайындау немесе сақтау;
- ҚР мемлекеттік лауазымын немесе ҚР субъектісінің мемлекеттік лауазымын атқаратын адамды өзінің лауазымдық міндеттерін атқару кезеңінде осы бапта көрсетілген және қылмыс болып табылатын іс-әрекеттер жасады деп көрінеу жалған айыптау;
- көрсетілген іс-әрекеттерді ұйымдастыру және дайындау, сондай-ақ оларды жүзеге асыруға арандату;
- көрсетілген іс-әрекеттерді қаржыландыру не оларды ұйымдастыруға, дайындауға және жүзеге асыруға, оның ішінде оқу, полиграфиялық және материалдық-техникалық базаны, телефондық және байланыстың өзге де түрлерін ұсыну немесе ақпараттық қызметтер көрсету жолымен өзге де жәрдемдесу

Бағыты бойынша:

- экономикалық (бір ғана меншік түрін орнату, бәсекелестікті болдырмау және т.б.);
- рухани (басқа мәдениет өкілдерінің жетістіктерін теріске шығару);
- экологиялық (табиғатты қорғау саясатына қарсы шығу);
- діни (басқа конфиссия өкілдеріне деген жеккөрушілік);
- ұлттық (басқа ұлттардың қызығушылықтары менн құқықтарын теріске шығару);
- саяси (үкіметтік құрылымдар, мемлекеттік қызметтерге қарсы шығу).

Іс-әрекеттердің масштабына байланысты:

- -мемлекетішілік (өз ұлтына репрессия жасау);
- -мемлекетаралық (өз нормалары мен принциптерін әлемдік масштабға орнатуға тырысу).

Өкілетті құрылымдарға байланысты:

- -мемлекеттік (репрессияның өкілетті құрылымдары арқылы орындалады);
- -мемлекетке оппозициялық (антирежимдік топтар; терактар).

Экстремизмнің негізгі түрлері

	Экстремизм түрі	Экстремизмнің берілген түріні негізгі түсінігі
	Сепаратизм	Мемлекеттің бір бөлігін бөліп алып, оны жаңа тәуелсіз мемлекетке немесе автономды бөлікке айналдыруға ұмтылу
	Ксенофобия	Басқа мәдениет, ұлт, мемлекет өкілдеріне деген төзімсіздік
	Ұлтшылдық	Белгілі бір ұлттың артық екендігін айтуға негізделетін идеология, саяси көзқарастар жүйесі
	Шовинизм	Басқа ұлт өкілдерін кемсіту, эксплуатациялау және дискриминациялау мақсатында қандай да бір басқа ұлттық артықшылығын насихаттайтын идеология
	Расизм/нәсілшілдік	Әр түрлі нәсілдердің физикалық және психикалық кемелденбегенін насихаттайтын идеология. Халықты «жоғарыдағылар» және «төмендегілер», «кемелденгендер» мен «кемелденбегендер» деген сияқты топтарға жіктеу, нәсілдік тиістілікке байланысты нәсілдік дискриминация, ұлт геноциді үшін пайдаланылады.
	Фашизм	Әскери расизм, «басқа» ұлттық және әлеуметтік топтарға ксенофобиядан басталып, геноцидке, мистикалық дұшпандыққа, тоталитарлық мемлекетке табынуға ауысатын әлеуметтік-саяси қозғалыстардың жалпы атауы.
	Терроризм	Тек зорлық-зомбылық құралдарын қолдану арқылы орындалатын саясат.

Экстремизм түрлері

Экстремистік көріністердің қолдану саласының сипаты бойынша келесі жіктелуін де бөліп көрсетуге болады: саяси сипатта; экономикалық сипатта; діни сипатта және психологиялық сипатта.

Ең үлкен қауіп – саяси экстремизм. Бұл жағдайда «оң» және «сол» экстремизм ерекшеленеді. Солшыл экстремизмнің негізі – анархизмнің революциялық идеялары, өзін ең дәйекті экспрессор және жұмысшы бұқараның, барлық аз қамтылған және кедей адамдардың қорғаушысы ретінде анықтайды. Оңшыл экстремизмге (фашистік, неофашистік, ультра оңшыл, ұлтшыл, нәсілшіл қозғалыстар, ұйымдар мен партиялар) келетін болсақ, ол халықаралық деңгейде ұйымшылдық пен үйлесімділіктің жоғары деңгейімен сипатталады.

Діни экстремизм конфессиялық принцип бойынша тәуелсіз теократиялық мемлекет немесе аумақтық автономия құруға арналған діни ұстанымдармен алдын ала анықталады.

Ұлттық экстремизм әдетте саяси экстремизмнің және діни экстремизмнің элементтерімен сипатталады. Алайда, саяси экстремизм таза діни идеяны болмаса да,жалған діни идеяны жүзеге асырады. Осылайша, кез-келген экстремистік қозғалыс өзара байланысты және әр нақты жағдайда күшті немесе әлсіз көрінетін әртүрлі элементтерді қамтиды.

КАК ПОНЯТЬ, ЧТО МАТЕРИАЛ ЭКСТРЕМИСТСКИЙ?

МАТЕРИАЛ, НА КОТОРЫЙ ТЫ НАТКНУЛСЯ В СЕТИ:

1. *содержит публичное оправдание терроризма и иной террористической деятельности*

2. *призывает к социальной, расовой, национальной или религиозной розни (важно, что «рознь» – гораздо более широкое понятие, чем ненависть или вражда)*

3. *пропагандирует исключительность, превосходство либо неполноценность человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии*

4. *пропагандирует или публично демонстрирует нацистскую атрибутику или символику либо атрибутику или символику, сходные с нацистской атрибутикой или символикой до степени смешения, либо публично демонстрирует атрибутику или символику экстремистских организаций*

СОМНЕВАЕШЬСЯ? СВЕРЬСЯ С ФЕДЕРАЛЬНЫМИ СПИСКАМИ:

1. Федеральный список экстремистских материалов
2. Список экстремистских и террористических организаций
3. Единый федеральный список организаций, в том числе иностранных и международных организаций, признанных в соответствии с законодательством РФ террористическими

НЦПТИ

Кибертерроризм

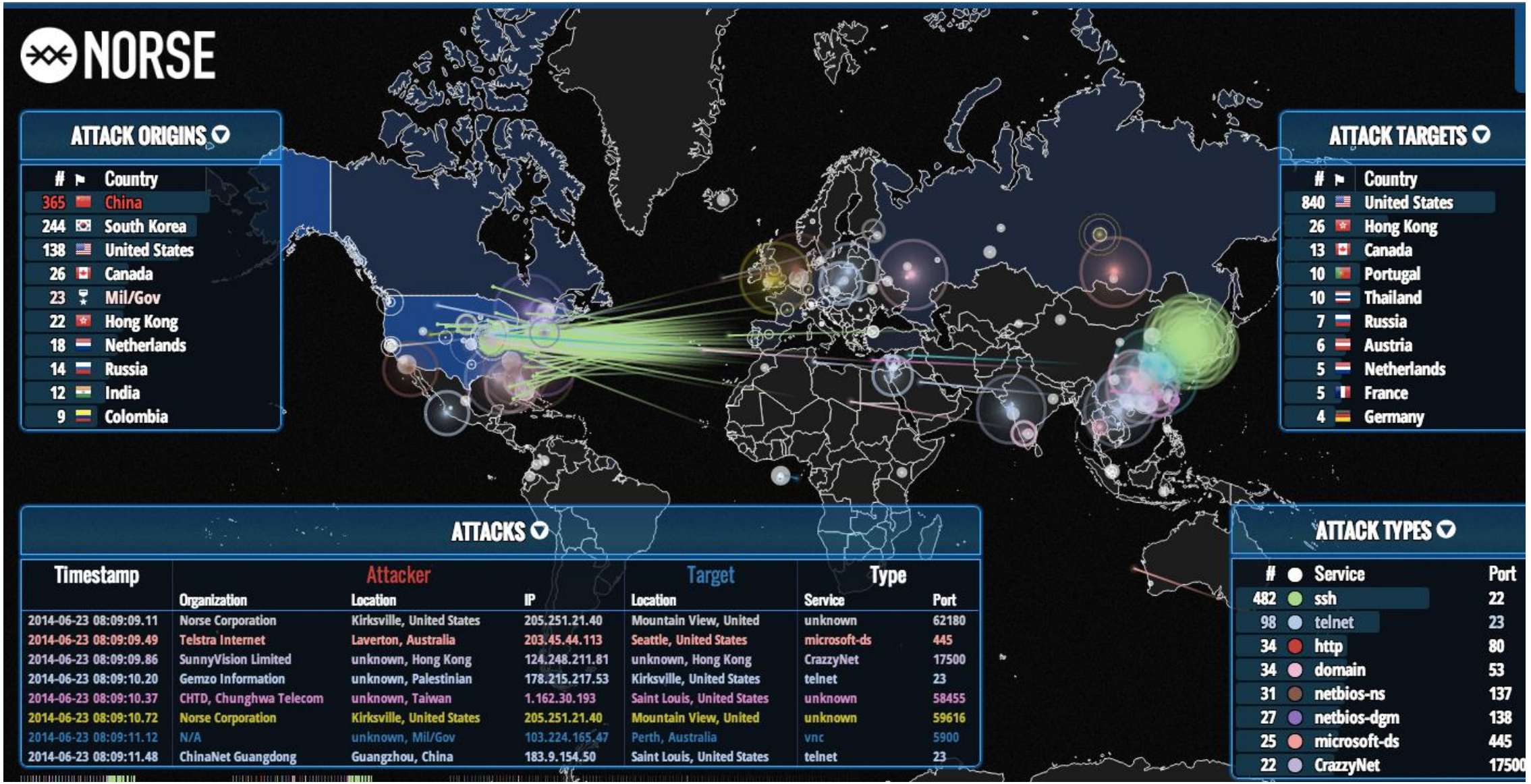
- Компьютерлік технология дамығандықтан, ақпараттарды электронды түрде өңдеп, қылмыстық мақсаттар үшін пайдаланатын «кибертерроризм» атты қылмыстың жаңа түрі пайда болды.
- Кибертерроризм тізіміне жасырын ақпараттар мен мемлекеттік құпияларға қол жеткізу мақсатында ғаламтор желісін пайдалану, сондай-ақ әртүрлі вирустарды, жаппай деструктивті сипаттағы материалдар мен ақпараттарды тарату мен насихаттау кіреді.

Кибертерроризмнің мақсаттары

Кибертерроризмнің әрекеттері:

- компьютерлік жүйелерді бұзу және жеке және банктік ақпаратқа, әскери және мемлекеттік құпия мәліметтерге қол жеткізу;
- жабдықтар мен бағдарламалық жасақтаманы істен шығару, кедергілер жасау, электр желілерінің жұмысын бұзу;
- компьютерлік жүйелерді бұзу, вирустық шабуылдар, бағдарламалық бетбелгілер арқылы деректерді ұрлау;
- Құпия ақпараттың ашық қол жетімділікке ағуы;
- басып алынған БАҚ арналары арқылы жалған ақпарат тарату; байланыс арналарының жұмысын бұзу және т.б. бағытталады.

Қажетті мақсаттарға жету үшін кибертеррористтер компаниялар мен ұйымдардың компьютерлік жүйелерін бұзу үшін қолданылатын арнайы бағдарламалық жасақтаманы қолданады, компаниялар мен ұйымдардың қашықтағы серверлеріне шабуыл жасайды.


NORSE
ATTACK ORIGINS
Country
365 China
244 South Korea
138 United States
26 Canada
23 Mil/Gov
22 Hong Kong
18 Netherlands
14 Russia
12 India
9 Colombia
ATTACK TARGETS
Country
840 United States
26 Hong Kong
13 Canada
10 Portugal
10 Thailand
7 Russia
6 Austria
5 Netherlands
5 France
4 Germany
ATTACKS
Timestamp | Attacker | | | Target | Type | |
Organization | Location | IP | Location | Service | Port
2014-06-23 08:09:09.11 | Norse Corporation | Kirksville, United States | 205.251.21.40 | Mountain View, United | unknown | 62180
2014-06-23 08:09:09.49 | Telstra Internet | Laverton, Australia | 203.45.44.113 | Seattle, United States | microsoft-ds | 445
2014-06-23 08:09:09.86 | SunnyVision Limited | unknown, Hong Kong | 124.248.211.81 | unknown, Hong Kong | CrazzyNet | 17500
2014-06-23 08:09:10.20 | Gemzo Information | unknown, Palestinian | 178.215.217.53 | Kirksville, United States | telnet | 23
2014-06-23 08:09:10.37 | CHTD, Chunghwa Telecom | unknown, Taiwan | 1.162.30.193 | Saint Louis, United States | unknown | 58455
2014-06-23 08:09:10.72 | Norse Corporation | Kirksville, United States | 205.251.21.40 | Mountain View, United | unknown | 59616
2014-06-23 08:09:11.12 | N/A | unknown, Mil/Gov | 103.224.165.47 | Perth, Australia | vnc | 5900
2014-06-23 08:09:11.48 | ChinaNet Guangdong | Guangzhou, China | 183.9.154.50 | Saint Louis, United States | telnet | 23
ATTACK TYPES
Service Port
482 ssh 22
98 telnet 23
34 http 80
34 domain 53
31 netbios-ns 137
27 netbios-dgm 138
25 microsoft-ds 445
22 CrazzyNet 17500

Кибертеррористер бомба қоймайды, тұтқындарды алмайды. Олар компьютерлік құралдармен қауіп төндіреді: компанияның ірі компьютерлік желісінің істен шығуы, банк клиенттерінің деректерін жою, зауыттар мен электр станцияларының жұмысын бұзу және т.б. сатып алу мақсатында.

Қойылған мақсаттарға жету үшін әртүрлі әдістерді қолдануға болады:

құпия ақпаратпен мемлекеттік және әскери мұрағаттарға, банктік шоттар мен төлем жүйелерінің деректемелеріне, жеке деректерге заңсыз қол жеткізу;

инфрақұрылым объектілеріне олардың жұмыс қабілеттілігіне ықпал ету үшін жекелеген құрауыштарды істен шығарғанға дейін және тіршілікті қамтамасыз ету жүйелерін толық тоқтатқанға дейін бақылауды жүзеге асыру;

әртүрлі үлгідегі зиянды бағдарламаларды енгізу жолымен ақпаратты, бағдарламалық құралдарды немесе техникалық ресурстарды ұрлау немесе жою; экономикалық немесе әлеуметтік-саяси жағдайды тұрақсыздандыруға әкеп соғуы мүмкін шабуылдар жасаудың жалған қатерлері.

Осы және ұқсас операцияларды жүргізу әдістері әртүрлі компьютерлік желілерде қолданылатын ақпараттық қауіпсіздік жүйелерінің дамуына байланысты үнемі өзгеріп отырады. Ақпараттық инфрақұрылымның даму деңгейі мен хакерлік шабуылдар саны арасындағы байланыс анықталды. Жаһандану деңгейі және осы аймақтағы әртүрлі процестерді автоматтандыру жүйелерін пайдалану неғұрлым жоғары болса, террористік кибершабуылдардың ықтималдығы соғұрлым жоғары болады.

Кибертерроризмге қарсы күрес

Мемлекет ғаламтор кеңістігіндегі деструктивті сайттарды, порталдарды, интернет-парақшаларды, форумдарды анықтау мақсатында үнемі мониторинг жүргізіп отырады. Мониторинг барысында айқындалған деструктивті немесе діни терроризмнің нышандары бар интернет-ресурстарына дінтану сараптамасы жүргізіледі.

Сараптама қорытындысының негізінде сот жүргізіліп, экстремистік мазмұны айқындалған ресурсты Қазақстанның ақпараттық кеңістігінде таратуды тоқтату немесе толықтай жабу жөнінде шешім қабылданады.

Кибертерроризмге қарсы әрекет етудің бір әдісі – желідегі деструктивті мазмұндағы материалды жедел түрде жою және оған кіру жолдарын жабу.

Киберсоғыс

Киберсоғыс (ағыл. cyberwarfare) - кибернетикалық кеңістіктегі (киберкеңістіктегі) қарама-қайшылық (соғыс) және текетірес, соның ішінде интернеттегі компьютерлік текетірес, ақпараттық соғыс түрлерінің бірі. Ең алдымен компьютерлік жүйелерді тұрақсыздандыруға және мемлекеттік мекемелердің, қаржы және бизнес орталықтарының Интернетке қол жетімділігін тұрақсыздандыруға және күнделікті өмірде Интернетке сүйенетін елдер мен мемлекеттердің өмірінде тәртіпсіздік пен хаос құруға бағытталған. Мемлекетаралық қатынастар мен саяси қарама-қайшылық көбінесе интернетте кибер соғыс және оның құрамдас бөліктері түрінде жалғасады: вандализм, үгіт-насихат, тыңшылық, компьютерлік жүйелер мен серверлерге тікелей шабуылдар және т.б.

Киберсоғыс тарихы

АҚШ үкіметінің қауіпсіздік жөніндегі сарапшысы Ричард Кларк өзінің «Киберсоғыс" атты кітабында (ағылш. CyberWarfare) (2010 жылдың мамыр айында шыққан) "кибер соғыс — бір мемлекеттің басқа мемлекетке зиян келтіру немесе жою мақсаттарына жету үшін олардың компьютерлеріне немесе желілеріне енетін әрекеті« деген анықтама береді. Британдық The Economist журналы киберкеңістікті "Жер, Теңіз, ауа және ғарыштан кейінгі соғыстың бесінші аймағы"деп сипаттайды.

Киберкеңістіктегі соғыс қимылдары саласындағы алғашқы қадамдар 2000 жылдардың басында жасалды. Келесі құрылымдар құрылды:

2005 жыл: Еуропалық Одақтың желілік және ақпараттық қауіпсіздік агенттігі

2010 жыл: АҚШ кибернетикалық қолбасшылығы.

2014: ақпараттық операциялар әскерлері

Сипаттамалық белгілері

Компьютерлік технологиялардың таралуымен көптеген азаматтар, кәсіпорындар мен мемлекеттік мекемелер күнделікті өмірде Интернетке тәуелді бола бастады. Интернетті басқа мемлекеттің компьютерлік жүйелеріне шабуыл жасау үшін пайдалану оның экономикасына айтарлықтай зиян келтіріп, елдің күнделікті өмірінде алауыздық тудыруы мүмкін. Өткен кибершабуылдардан айырмашылығы, қазір кибер соғыс елдің ұлттық қауіпсіздігіне қауіп төндіреді және оны көптеген адамдар мемлекет қауіпсіздігіне елеулі қауіп ретінде қабылдайды.Сонымен қатар, көптеген елдердің барлау ұйымдары интернетте тыңшылық жасайды: олар ақпарат жинайды, басқа мемлекеттердің компьютерлік жүйелерін бұзады, диверсиялық қызметпен және экономикалық тыңшылықпен айналысады.

Жаңа технологиялардың дамуына байланысты кибер соғыс деңгейі үнемі жетілдіріліп отырады. Кейбір мемлекеттер кибершабуылдан қорғауға тиісті назар аудара бастайды — олар қорғаныс жүйелерін ұйымдастыруға қажетті қаражат бөледі және арнайы бөлімшелерді қолдайды, олардың негізгі міндеті елдің интернет қауіпсіздігін және шабуылдардан қорғауды жетілдіру болып табылады.

Киберсоғыс түрлері

Мақсаттары мен міндеттеріне сәйкес киберкеңістіктегі әскери әрекеттер екі санатқа бөлінеді: *тыңшылық және шабуылдар*.

Тыңшылық немесе - шет мемлекеттердің органдарының (олардың агенттерінің) заңсыз барлау қызметі, бұл, әдетте, басқа мемлекеттердің арнайы қызметтерінің ресми құпия ақпаратты (мемлекеттік құпияны) ұрлауын білдіреді.

Тыңшы-басқа тараптың пайдасына қақтығысушы тараптардың бірі туралы жасырын ақпарат жинаумен айналысатын адам.

Шпион, әдетте, қарсылас туралы ақпаратты әртүрлі құпия тәсілдермен (қарау, тыңдау, соның ішінде арнайы техникалық құралдарды қолдану) немесе қарсыластың жағына енгізу арқылы, яғни өзін оның жақтаушысы ретінде көрсету арқылы немесе осы екі жолдың тіркесімі арқылы алатын адам деп аталады. Шпионды шетелдік барлаудың толық уақытты қызметкері де, шетелдік барлаумен жалданған және оған жұмыс, қызмет немесе жеке байланыстар арқылы белгілі құпия ақпаратты беретін мемлекет азаматы деп атауға болады.

Шабуылдар

Сарапшылар интернеттегі шабуылдардың келесі түрлерін ажыратады:

Вандализм-интернет беттерін бүлдіріп, мазмұнын басқаларды келеке ету немесе өзге нәрсені насихаттайтын суреттермен алмастыру үшін хакерлердің интернетті пайдалануы.

Насихат – ақпарат беру сипатындағы өтініштерді тарату немесе насихатты басқа интернет-беттердің мазмұнына енгізу.

Ақпарат жинау-құпия ақпаратты жинау және/немесе оны басқа мемлекетке пайдалы жалған ақпаратпен алмастыру үшін жеке беттерді немесе серверлерді бұзу.

Сервистің істен шығуы-сайттардың немесе компьютерлік жүйелердің жұмыс істеуін бұзу үшін әртүрлі компьютерлерден шабуылдар.Жабдықтың жұмысына араласу-азаматтық немесе әскери жабдықтардың жұмысын бақылаумен айналысатын компьютерлерге шабуыл жасау, бұл оның ажыратылуына немесе бұзылуына әкеледі.

Инфрақұрылым пункттеріне шабуылдар-қалалардың тіршілігін қамтамасыз ететін компьютерлерге, олардың телефон жүйелері, сумен жабдықтау, электр энергиясы, өрт күзеті, Көлік және т. б. инфрақұрылымдарына шабуылдар.

Экстремизмге қарсы іс-шара

- көптеген сарапшылар интернеттегі экстремистік сипаттағы қылмыстардың өте жоғары кідірісін атап өтеді. Қазіргі уақытта олардың шамамен 30-35% - ы анықталды деп болжануда. Мұның негізгі себебі - интернет желісінде экстремизмге қарсы іс-қимылды ресурстық қамтамасыз ету жүйесінің жеткіліксіздігі. Экстремизмге қарсы іс - қимылдың тиімділігін қамтамасыз ету үшін үш шарт қажет:
- интернет желісінде экстремизмге қарсы іс - қимылдың құқықтық негізі;
- жедел бөлімшелер қызметкерлерінің біліктілігі;
- материалдық-техникалық қамтамасыз ету.
- Өкінішке орай, қазіргі уақытта осы жағдайлардың әрқайсысы үшін тапшылық байқалады. Болашақта ақпараттық желілер мен ресурстардағы экстремистік топтар мен қозғалыстардың одан да көп белсенділігі артады деп болжауға болады.

- Экстремистік ұйымдар мен топтар түрлі танымал әлеуметтік желілер –WhatsApp, Youtube, Viber, ВКонтакте, Facebook, Twitter арқылы деректі фильмдерді, аудио және бейне – хабарламалар мен үгіт-насихаттарды жиі пайдаланады. Әлеуметтік желілердегі экстремизмді насихаттаудың өзіндік ерекшелігі бар, өйткені жеке ақпарат көбінесе әлеуметтік желілерде көрсетіледі, демек, белгілі бір жас тобындағы адамдардың санасына максималды әсер ету үшін экстремистік материалдарды мақсатты түрде тарату мүмкін. Әлеуметтік желі өзінің жалдау және насихаттау функциясында баспа басылымдары мен қарапайым сайттардан асып түскенін атап өткен жөн. Олардың артықшылығы – жалдаушы мен оның ықтимал құрбаны арасындағы жеке, қауіпсіз және жиі жасырын қарым-қатынас мүмкіндігін арттыру. Сондай-ақ, психологиялық тұрғыдан, пайдаланушы теледидарға, газеттерге немесе сайттарға қарағанда әлеуметтік желілерден алынған ақпаратқа көбірек сенетінін атап өткен жөн. Дәл осы мақсатты экстремистер белсенді қолданады.
- Әлеуметтік желілердегі аккаунттардың көпшілігі екі түрге бөлінетіні анық. Біріншісі кейіннен танымал бола бастаған жаңалықтар арналарының ең өзекті басылымдарын анықтайды. Екіншісі бұл жазбалармен,фотосуреттер және бейне материалдармен бөлісетін жеке адамдардың парақшасы, сондай-ақ экстремистік сипаттағы хабарламалар мен дәлелдер жиі жарияланатын пайдаланушылардың жеке парақтары.

Әлеуметтік желілердегі ақпараттық экстремизм көп қырлы тұжырымдама ретінде ұсынылады, оның негізгі мақсаты интернетте жасанды түрде жасалған қауесеттер арқылы көпшіліктің санасын айла-шарғы жасау болып табылады, оны көптеген ғалымдар мен сарапшылардың пікірінше, қоғамның тұрақты өмір сүруіне қауіп ретінде ғана емес, сонымен бірге еліміздің ақпараттық қауіпсіздігі ретінде де қарастыруға болады. Әлеуметтік желі мен ақпарат саласындағы қалыптасқан жағдайды талдау қоғам әлі күнге дейін патогендік ақпараттық технологиялар туралы жеткіліксіз деңгейде хабардар екенін айқын көрсетеді.

Қорытынды

Сонымен қатар, интернет желісі экстремистерді қолдауда маңызды рөл атқаратын қолдаушылар мен көмекшілерді тарту үшін қолданылады. Экстремистер тиісті ақпаратты беру жылдамдығында электронды баспа және БАҚ-пен салыстырғанда интернет мүмкіндіктерін кеңінен пайдаланады. Экстремизм әртүрлі жастағы аудиторияның санасына әсер ету арқылы әлеуметтік желілерде кеңінен таралды. Қазіргі уақытта құқық қорғау органдары интернет-ресурстарда, әсіресе әлеуметтік желілерде экстремистік идеяларды, көзқарастар мен үндеулерді белсенді түрде анықтап жатыр.

Назарларыңызға рақмет!