Koostanud: valitsuse kommunikatsioonibüroo
Uuendatud: 15.02.2019

Juhend inforünnakutega toimetulemiseks

Sissejuhatus

Mõisted nagu valeuudised, desinformatsioon ja mõjutustegevus on murdnud kõigi suuremate väljaannete veergudele ja sotsiaalmeedia uudisvoogudesse. Selles juhendis on teadlikult välditud valeuudiste ja valeinfo mõisteid, sest need ei erista tahtlikku infoga manipuleerimist inimlikest vigadest või satiirist. Siin on kasutatud läbivalt desinformatsiooni (lühidalt desinfo) mõistet. Desinformatsioon on teadlik – enamasti planeeritud ja koordineeritud – tegevus infokeskkonna moonutamiseks, et saavutada oma strateegilisi eesmärke. Sageli on selleks eesmärgiks valearusaamade külvamine, usalduse kahandamine riigiinstitutsioonide ja meedia vastu, üldsuse segadusse ajamine või eri ühiskonnagruppide polariseerimine. Viimasel ajal üha enam ka valimistesse sekkumine.

Eesti riigiaparaat toimib detsentraliseeritult, mis tähendab, et iga ministeerium ja asutus vastutab enda õuel toimuva eest. See kehtib ka informatsioonilise mõjutustegevuse vallas. Meil on asutusi, kes sel teemal süsteemselt silma peal hoiavad, ent me kõik peame suutma üksikute juhtumitega ise toime tulla. Selle juhendi mõte ongi anda esmased näpunäited desinfo äratundmiseks ning (vajadusel) sellele reageerimiseks. Dokumendi lõpust leiab kolm lisa: 1) levinumad mõjutusmeetodid; 2) näpunäited võõrastele ajakirjanikele vastamiseks ja allikakriitika ABC; 3) botid.

Selle juhendi koostamisel on võetud suuresti eeskuju Rootsi tsiviilkaitseameti (MSB) ja Lundi ülikooli koostöös 2018 suvel valminud põhjalikust käsiraamatust.[1]

1. Desinforünnakuteks valmistumine

Selleks, et desinforünnakutele adekvaatselt, kiiresti ja tõhusalt vastata ning nende negatiivset mõju leevendada, tuleb oma inimesed selleks eelnevalt ette valmistada (st tõsta nende teadlikkust ja neid koolitada) ning leppida kokku, kes millist rolli kannab. Ettevalmistustöö võib jagada laias laastus kaheks:

1. asutuse haavatavuste väljaselgitamine ning desinformatsiooni alase teadlikkuse tõstmine;
2. (valve)narratiivide ja -sõnumite ettevalmistamine.

<u>Haavatavuste väljaselgitamine ja teadlikkuse tõstmine</u>
Oma asutuse haavatavuste väljaselgitamine on üks olulisemaid elemente desinforünnakute vastase valmisoleku tõstmisel. Kuivõrd desinforünnakute üks sagedastest eesmärkidest on ohvri usaldusväärsuse kahandamine, tasub keskenduda tegevustele, mis kindlustavad ja tõstavad asutuse usaldusväärsust nii partnerite ja klientide silmis kui ka ühiskonnas laiemalt. Mida enam inimesed asutust usaldavad, seda keerulisem on seda desinforünnakuga tasakaalust välja lüüa.

Kommunikatsiooniinimesena saad astuda mitmeid samme, et enda asutust paremini ette valmistada. Esiteks on oluline, et arutaksid neil teemadel oma asutuse juhtkonnaga ning jagaksid asjakohast infot ka teiste kolleegidega. Teiseks on kommunikatsioonitöötajal asutuses oluline nõuandev roll. Kui su asutus sattub desinforünnaku alla, siis oled sina esimeste seas, kelle poole nõu küsimiseks pöördutakse. Seetõttu tasub luua enda ümber võrgustik sarnases vallas tegutsevatest inimestest, kellega vajadusel nõu pidada ning kogemusi ja õppetunde vahetada. Sellega saab sind aidata ka riigikantselei strateegilise kommunikatsiooni meeskond.

[1] MSB käsiraamatuga saab tutvuda aadressil www.msb.se/RibData/Filer/pdf/28698.pdf.

Narratiivide ja sõnumite ettevalmistamine
Kriisiolukorras, mida tõsine ja koordineeritud desinforünnak kahtlemata on, on kõigil käed ja jalad tööd täis ning sõnumite koostamine ja heakskiitmine võib liialt aega võtta. Samal ajal on oluline oma tõene versioon toimunust võimalikult kiiresti välja saada, sest see annab edasistele sõnumitele ja järgnevatele avalikele aruteludele tooni. Seetõttu tasub üldised sõnumid ja jutupunktid, mida saab vastavalt olukorrale kohandada, varem ette valmistada. Neid sõnumeid koostades pea silmas oma asutuse väärtusi ja olulisemaid haavatavusi. Abiks on see, kui mõtled, milliseid lugusid on su asutuse kohta varem levitatud.

2. Inforünnakutele reageerimine

Nagu enamasti elus, pole inforünnakutele reageerimiseks ühte lahendust, mis töötaks igas olukorras. Nii inforünnakute tüübid kui ka kõigi asutuste haavatavused on erinevad. Lisaks on oluline meeles pidada seda, et igale inforünnakule polegi mõistlik vastata. Teatud olukordades võib see negatiivseid sõnumeid vaid võimendada või neid legitimeerida. Alljärgnevalt on toodud neli etappi, millega reageerimisel arvestada. Päriselus võib nende järgnevus erineda ning iga olukorda tuleb alati eraldi hinnata.

1. Olukorra hindamine. See on neutraalne samm, mis on vajalik eeskätt asutusele endale, et saada toimuvast ülevaade. Samal ajal saadab see teistele esialgse signaali, et oled toimunust teadlik ja tegeled detailide väljaselgitamisega.
    a. Kaardista olukord: Selgita võimalikult kiiresti välja, mis toimus. Oluline on aru saada, kas tegemist on tõesti desinforünnaku või hoopis millegi muuga.
    b. Käivita (sotsiaal)meediaseire: Kuivõrd me räägime infotandril toimuvast, peame selle ohjamiseks omamama inforuumist võimalikult head pilti. Selleks tuleb sisse seada temaatiline (sotsiaal)meediaseire.
    c. Kontrolli fakte: Kontrolli, kas asutuse vastu välja käidud sõnumites olevad väited vastavad tõele.
    d. Teavita osapooli: Jaga toimunu kohta infot kolleegidele ja olulisematele partneritele. Mida kiiremini nad toimunust asutuse enda käest teada saavad, seda parem.
    e. Ole läbipaistev: Kaasa ajakirjanikke, eksperte ja teisi majaväliseid partnereid, kes saavad toimunut neutraalselt ja läbipaistvalt hinnata ja/või kajastada.
    f. Anna välja esialgne sõnum: Saada oma sihtrühmale sõnum, et oled toimunust teadlik ja tegeled olukorra lahendamisega. See annab natuke aega, et töötada välja ammendavam vastus.
2. Avalikkuse ja olulisemate partnerite teavitamine. See samm on vajalik avalike arutelude ohjamiseks.
    a. Anna välja ametlik sõnum: Ole võimalikult läbipaistev, jaga oma sihtrühmaga toimunu kohta nii palju neutraalset ja tõest informatsiooni kui tarvis.
    b. Paranda faktivigu: Kui su asutuse kohta levitatakse desinforünnaku ajal väärat informatsiooni, siis lükka see asjakohaste faktidega ümber. Korduma kippuvate küsimuste rubriik on üks klassikaline, aga hea näide, kuidas teha seda nii, et ei peaks vastama igale üksikule päringule.
    c. Viita: Kui avaliku aruteluga on omal initsiatiivil liitunud asutusevälised asjatundjad, kes on teinud häid ja usaldusväärseid väljaütlemisi, siis viita võimalusel neile.
    d. Ära unusta oma väärtusi: Tuleta oma sõnumitega meelde, millised on su asutuse väärtused, mille eest te seisate.
3. Proaktiivne kommunikatsioon. Selles etapis võtad endale selge positsiooni ja levitad seda proaktiivselt.
    a. Astu dialoogi: Suhtle olulisemate partnerite ja sihtrühmadega ning kaasa nad olukorra lahendamisse.

   b. Tee kogu olulisem info lihtsasti leitavaks ja kättesaadavaks: Koosta infomaterjal, kus on kajastatud tõene ja faktipõhine info, mis toetab su seisukohti, ning riputa see enda veebilehele. Sellest saab punkt, millele saad edaspidi viidata. Veendu, et su leht oleks otsingumootoritele optimeeritud (ingl k *Search Engine Optimisation*, SEO), sest suurem osa inimestest ei jõua su lehele mitte otse, vaid otsingumootori (enamasti Google'i) kaudu.
   c. Jutusta lugusid: Pakenda oma sõnumid lugudesse, mis kõnetavad su sihtrühma. Su sõnumid peaksid andma lugejale lihtsasti mõistetava ülevaate toimunust, millega nad suhestuvad, ning olema lihtsalt kontrollitavad. Faktid ja narratiivid täiendavad teist.
   d. Kasuta arvamusliidreid: Võta ühendust arvamusliidritega, kes saavad aidata su sõnumit sihtrühmadele edasi anda.
   e. Optimeeri: Kriisiolukorras ei ole enamasti aega, et uusi kanaleid sisse töötada. Selle asemel kasuta oma sõnumite levitamiseks olemasolevaid sündmusi, algatusi, veebilehti (nt Wikipedia, mis on otsingumootorites kõrgel kohal) jm võimalusi.
4. Vastutegevus. Sellega astud otseselt vastu oma ründajale.
   a. Ignoreeri: Mõnikord on parim üldse mitte reageerida. See on mõistlik olukorras, kus desinforünnak on küll toimunud, kuid selle levi on väga piiratud ning mõju väike.
   b. Raporteeri: Kui su asutuse ründaja rikub Eesti seadusi või muid reegleid, siis teavita sellest politseid või teisi asjakohaseid asutusi. Seda võimalust tuleks kasutada aga tõesti vaid sel juhul, kui oled veendunud, et seadusi või reegleid on rikutud, mitte kellegi suukorvistamiseks.
   c. Lase kustutada: Kommunikatsioonieksperdina on ülioluline mõista, et me elame vabas ühiskonnas, mille üks alustalasid on sõnavabadus. Erandlikel juhtudel võib siiski olla põhjendatud kellegi postitatud sisu või konto kustutamine veebiplatvormilt. Selleks tuleb platvormile (olgu selleks nt Google, Facebook, Instagram või Youtube) teada anda. See samm on aga õigustatud vaid juhul, kui rikutud on Eesti seadusi või platvormi enda reegleid. Kuivõrd kõigi levinumate platvormide kodukorrad on mõnevõrra erinevad ning ajas muutuvad, ei ole mõistlik neid siia juhendisse kirja panna. Need on veebist lihtsalt leitavad.
   d. Paljasta: Teatud olukordades võib strateegiliselt parim valik olla rünnaku autori paljastamine, süü omistamine (ingl k *attribution*). Seda tasub kaaluda vaid juhul, kui ründaja on (piisava veendumusega) teada ning potentsiaalne kahju, mis sellega kaasneda võib, ei kaalu üle võimalikku positiivset mõju.

3. Õppetunnid tulevikuks

Kriisiolukorras on oluline keskenduda toimuva lahendamisele, ent kui tavaolukord on taastatud, siis on mõistlik võtta hetk, et vaadata toimunule tagasi ja tehtud sammud rahulikult uuesti läbi käia. See aitab tulevasteks desinforünnakuteks paremini valmistuda ning mõnda ehk isegi ära hoida.

Kontrollnimekiri, mis aitab seda teha:

1. Kirjelda:
   a. Kirjelda toimunu tausta, põhjuseid ja juhtumi kulgu.
   b. Kes olid vahejuhtumiga seotud osapooled? Väldi spekulatsiooni, kui pole kindel.
   c. Milliseid mõjutustehnikaid kasutati?[2]
   d. Milliseid narratiive kasutati ja keda nendega kõnetada üritati?
   e. Milliseid haavatavusi ära kasutati?
   f. Kas toimunu haakus ühiskonnas mõne päevakajalise teemaga?

[2] vt Lisa 1

2. Analüüsi:
    a. Millist mõju soovis ründaja saavutada? Millele tuginedes seda väidad?
    b. Kuidas rünnakule reageerisid? Miks just nii?
    c. Milline mõju oli valitud lahenduskäigul?
    d. Mis töötas hästi ning mida võinuks teha teisiti?
    e. Mis oleks juhtunud, kui poleks reageerinud?
    f. Millised on olulisemad õppetunnid, mille tulevikuks kaasa võtad?
3. Jaga:
    a. Kas kogusid usaldusväärseid tõendeid või muid andmeid, mida oma partneritega jagada?
    b. Aruta desinforünnaku mõju oma juhtide ning kolleegidega, jagage kogemusi.
    c. Jaga oma teadmisi ja kogemusi majaväliste partneritega, kes töötavad sarnases valdkonnas või puutuvad kokku sarnaste teemadega.

LISA 1. Levinud mõjutusmeetodid

Sotsiaalne ja kognitiivne mõjutamine:

- Varjatud reklaamid (ingl k *dark ads*): Need on reklaamid, mida näevad ainult inimesed, kellele need suunatud on. Kõigi teiste pilkude eest on need varjatud. Neid kasutatakse peamiselt infovälja moonutamiseks ja ühiskonna polariseerimiseks. Seni on neid enaim kasutatud Facebookis, kes need lõpuks keelas, tehes reklaamid nähtavaks kõigile.
- Trendiga kaasa minemine (ingl k *bandwagon effect*): Inimesed, kes kuuluvad mingis küsimuses enamuse hulka, ütlevad oma arvamusi julgemalt välja. Bottide[3] ja trollidega valitud sõnumite levikut võimendades saab tekitada tunde, et üks või teine arvamus on ühiskonnas väga populaarne. See omakorda võib teha laiemalt vastuvõetavaks seisukohad, mis seda tavaolukorras pole.
- Vaikimise spiraal (ingl k *spiral of silence*): Inimesed, kes tunnevad end olevat vähemuses, on vähem altid enda arvamust jagama. See mängib meie hirmule olla erinev või väljatõugatud.
- Kajakambrid ja infomullid (ingl k *echo chamber* ja *information bubble*): Inimesed koonduvad üldjuhul nende ümber, kes jagavad nende maailmavaadet. Seda nii päriselus kui ka internetis. Ühtlasi kiputakse tarbima infot, mis inimese maailmavaadet veelgi enam kinnitab, mistõttu ei pruugi inimesed teistsuguste arvamustega kuigi tihti kokku puutuda. Seda fenomeni võimendab sotsiaalmeedia platvormide toimimisloogika, mille eesmärk on inimestele võimalikult meelepärast informatsiooni pakkuda.

Eksitamine:

- Näiline sõltumatus (ingl k *shilling*): See on meetod, millega inimene üritab jätta muljet, et ta on sõltumatu, töötades samal ajal varjatult kellegi eesmärkide nimel. Igapäevaelust võib levinud näitena tuua kinnimakstud arvustajad, kes kommenteerivad internetis tooteid ja teenuseid. Desinformatsiooni vallas on parimaks näiteks palgalised trollid, kes kirjutavad etteantud teemadel (enamasti negatiivseid) kommentaare ja arvamusi.
- Jäljendajad ja isehakanud: Jäljendajad näitavad end kellegi teisena, võttes üle ohvri identiteedi. Isehakanud üritavad jätta muljet, et nad on eksperdid alal, millest nad ei pruugi tegelikult midagi teada.
- Libameedia: Desinformatsiooni võidakse levitada libameedia platvormidel, mis meenutavad aadressilt ja välimuselt mõnda olemasolevat uudisteportaali, aga pole seda tegelikult teps mitte.

Tehniline manipuleerimine:

- Botid: Botid on automatiseeritud arvutiprogrammid, mida juhivad inimeste kirjutatud koodiread. Osa neist on loodud ülla eesmärgiga arvutikasutajaid aidata, teised aga nende loojate eesmärkide täitmiseks, olgu need siis ärilised või poliitilised.
- Libakonto (ingl k *sockpuppets, fake account*): See on (sotsiaalmeedia) konto, mida kontrollib inimene, kes ei avalda oma tegelikku identiteeti ega eesmärki. Selliseid kontosid kasutatakse selleks, et ühineda veebis kogukondadega ning osaleda aruteludes, et süstida sinna eksitavat või vastuolulist infot. Kusjuures ühes grupis võidakse samaaegselt kasutada kahte vastanduvat seisukohta esindavat libakontot, et arutelu üles kütta. Pseudonüümide kasutamine on ajatu tava, ent libakontode loomine läheb vastuollu osade platvormide reeglitega. Näiteks Facebook on oma kodukorras libakontode tegemise, omamise ja haldamise selgesõnaliselt keelanud. Märgates Facebookis kontot, mida pead veenvatel alustel libakontoks, tasub sellest Facebookile teada anda.
- Ülirealistlikud videovõltsingud (ingl k *deepfakes*): Tänaseks on vabalt kättesaadav tehnoloogia, millega saab videopildis panna iga inimese ütlema mida tahes. Selleks on vaja vaid sobivat algmaterjali ehk korraliku kvaliteediga videot, kus inimene midagi räägib. Kuigi

[3] vt Lisa 2

selline manipuleerimine on varasemaga võrreldes oluliselt lihtsamaks muutunud, eeldab see siiani teatavaid tehnilisi oskusi ja aega, et lõpptulemus usutav jääks. Seni pole see meetod õnneks laiemat kasutust leidnud.
- Õngitsemine (ingl k *phishing*): Õngitsemine on inimeste trikitamine avaldama oma salasõnu ja muud tundlikku informatsiooni. Harilikult kasutatakse selleks e-kirju, millega võidakse mh jätta muljet, nagu pärineks see mõnelt usaldusväärselt teenusepakkujalt (nt Gmail või Facebook).

Desinformeerimine:
- Väljamõeldised: Teavet, millel ei pruugi olla mingit seost tegelikkusega, võidakse pakkuda usaldusväärse ja tõese sisu pähe. Näiteks võib tuua võltsitud kirjavahetuse, mille eesmärk on mõne avaliku elu tegelase maine kahjustamine.
- Manipuleerimine: Levinud mõjutusmeetod on infoga manipuleerimine. See tähendab, et tekstis, pildil või videos olevat sisu muudetakse. Samuti võib see tähendada uue info lisamist või olemasoleva valikulist kustutamist.
- Eksitav omistamine (ingl k *false attribution*): Ka faktiliselt korrektse infoga saab inimesi eksitada, kui seda kasutatakse näilise argumendina mitteseotud teemal. Sageli kasutakse valeuudiste veenvuse tõstmiseks fotosid sündmustelt, mis pole looga endaga kuidagi seotud.
- Satiir ja paroodia: Olgugi et satiir ja paroodia on üldjoontes ohutud meelt lahutavad žanrid, kasutatakse agressiivset huumorit ja liialdusi ka arvamuste naeruvääristamiseks ning inimeste ja sõnumite kritiseerimiseks.

Retoorika:
- Isiklik ründamine (lad k *ad hominem*): See on sõnumitooja ründamine, mustamine või naeruvääristamine, et tema sõnumi kaalu vähendada ning teda ennast heidutada.
- *Whataboutism*: See on tähelepanu probleemilt kõrvalejuhtimine, tõstes esile mõnda muud küsimust.
- Vastase ülekuhjamine (ingl k *gish-gallop*): See on vastase ülekuhjamine argumentide, väidete ja allikatega, mis ei ole tõesed arutelu teemaga seotud.
- Õlgmees (ingl k *strawman*): See on vastase diskrediteerimine, väites eksitavalt, et too on midagi öelnud ning seejärel seda väidet rünnates. Lühidalt – vastuvaidlemine väljamõeldud väi(de)tele.
- Arutelu kaaperdamine: See on käimasoleva aruteluga liitumine ning selle uuele teemale juhtimine.
- Väärdilemma (ingl k *false dilemma*): Sellega üritatakse jätta muljet, et valida on üksnes kahe (halva) alternatiivi vahel ning kuna üks neist on vastuvõtmatu, peab teine olema tõene.
- Libe nõlv (ingl k *slippery slope*): Põhjendamata väide, et mingit tegevust ei tohiks lubada, kuna see viib vältimatult teistele, vastuvõtmatutele või katastroofilistele tagajärgedele.

LISA 2. Botid

Botid on automatiseeritud arvutiprogrammid, mida juhivad inimeste kirjutatud koodiread. Osa neist on loodud ülla eesmärgiga arvutikasutajaid aidata, teised aga nende loojate eesmärkide täitmiseks, olgu need siis ärilised või poliitilised. Sotsiaalvõrgustikest kasutatakse botte enim Twitteris, aga need on üha enam levinud ka Facebookis.

Facebook
Facebookis on võimalik luua Messengeri vestlustes tegutsevaid heatahtlikke *chatbot*'e ehk juturoboteid, mis aitavad äridel parandada nende kliendisuhtlust. Juturobotid suudavad momentaalselt vastata lihtsamatele küsimustele, mis kasutajatel tekkida võivad, hoides kokku nii klienditeenindajate kui ka kasutajate endi väärtuslikku aega. Seda kõike eeldusel, et juturobot on piisavalt targalt kodeeritud. Kuna see on Facebookis võrdlemisi uus lahendus, on tänini kasutusel hulgaliselt kohmakaid juturoboteid, mis toovad kaasa vastupidise efekti ja kliendi pigem eemale peletavad.

Twitter
Twitteris kasutatakse samuti häid botte, kes jagavad näiteks kirjandusklassikute tsitaate või veebist leitud pilte, aga seal valmistavad tõsist peavalu pahatahtlikud botid, kes esinevad tegelike inimestena. Viimaseid kasutatakse enamasti selleks, et moonutada avalikus ruumis toimuvaid (poliitilisi) arutelusid, muuta näiliselt populaarseks valitud fraase või *hashtag*'e ehk teemaviiteid, võimendada sõnumeid ning rünnata teisi kasutajaid.

Twitteri botte on erinevat laadi. Jäljendajabotid üritavad sarnaneda tegelikele kasutajatele ja neid võib olla üsna keeruline ära tunda. Spämmibottide ainus ülesanne on aga infot võimalikult kiiresti ja paljudele inimestele levitada, mistõttu ei pruugi need isegi üritada reaalse kasutaja moodi välja näha ja neid on lihtsam ära tunda.

Õnneks on Twitter isegi mõistnud bottide kahjulikku mõju ja on asunud nende vastu võitlema. Ühest küljest arendab platvorm üha nutikamaks algorütme, millega botte ära tunda, ning samal ajal sulgevad nad regulaarselt kontosid, mis käituvad botilikult või ei vasta teistele reeglitele, millele kasutajad platvormiga liitudes alla on kirjutanud. Probleemi ulatuse illustreerimiseks olgu öeldud, et 2018 suve hakul kustutas Twitter keskmiselt enam kui miljon (liba)kontot päevas.

Kuus nõuannet, mis aitavad ära tunda kasutajaid, kes käituvad botilaadselt[4]:

1. Aktiivsus: Paljud botid on väga aktiivsed, postitades sadu kordi päevas või enamgi. Kui märkad kontot, mis postitab pikema perioodi jooksul enam kui 100 korda päevas, võid üsna kindel olla, et tegemist ei ole reaalse inimesega.
2. Personaalne info: Enamuste bottide kasutajanimed on automaatselt genereeritud. Ühtlasi on nende enesekirjeldused sageli kas tühjad või siis varastatud tegelikult kasutajatelt. Neil puudub sageli profiilipilt või siis kasutavad nad veebist varastatud pilte. Kui konto tekitab sinus kahtlust, siis tee tagurpidi pildiotsing, et näha, kas sama fotot on mujal kasutatud. Levinuim tööriist selleks on Google'i pildiotsing.
3. Võimendamine: Bottide üks levinumaid eesmärke on teiste kasutajate postituste võimendamine ehk siis nende jagamine ja tsiteerimine. Tüüpilise boti seinalt ei leia originaalseid postitusi, vaid valdavalt teiste postituste jagamisi ning tsitaate uudiste pealkirjadest ja mujalt.
4. Suhtlus teiste kasutajatega: Pööra tähelepanu sellele, milliste postituste ja kasutajatega konto suhestub. Botid on sageli osa koordineeritud võrgustikust, et võimendada teineteise postitusi, õngitsedes samal ajal uusi (tegelikest inimestest) jälgijaid. Ohumärk on see, kui

[4] Tõsikindlat pole võimalik tavakasutajaid bottidest eristada, küll aga saame kirjeldada boti-laadset käitumist.

konto alt on tehtud vaid üksikud postitused, aga need on väga populaarselt. Sellisel juhul võib olla tegu botivõrgustikuga ehk bottide kogumiga, kes jagab teineteise postitusi.

5. Konto loomise aeg: Paljud botid luuakse kindlaks eesmärgiks, mistõttu on nende kontod sageli alles hiljuti loodud. Samuti tasub ettevaatlik olla kontode suhtes, mille loomise aja ja esimese postituse aja vahel on ebaloogiliselt pikk aeg. Seda seetõttu, et aeg-ajalt taaskasutatakse vanu botte – varasemad postitused kustutatakse, et enda pahatahtlikku eesmärki varjata.
6. Keelekasutus: Botid kasutavad sageli masintõlget, et olla võimelised tegutsema samaaegselt mitmes keeles. Masintõlge on küll kõvasti arenenud, ent see sisaldab siiani pea alati vigu, ebatäpsusi ja kohmakaid konstruktsioone. Kui konto alt postitatakse pidevalt erinevates keeltes samasisulisi keeleliselt kohmakaid sõnumeid, on see järjekordne ohumärk.

Lisaks võid proovida sellist avalikku tööriista nagu Botcheck.me, mis suudab enam kui üheksal juhul kümnest tuvastada, kas kasutaja käitub botilikult või mitte. Selle kasutamiseks peab endal aga Twitteri konto olema.

Kui oled tuvastanud Twitteris konto, mida pead botiks (kes su asutust ründab), siis anna sellest platvormile teada. Selleks:

1. mine kontole, millest teada soovid anda;
2. vajuta ikoonile [kolm punkti või hammasratas];
3. vali menüüst *Report*;
4. vali *They are posting spam*.

LISA 3. Näpunäiteid võõrastele ajakirjanikele vastamiseks ja allikakriitika ABC

Päring tundmatult (välis)ajakirjanikult

Enne kui asud vastama tundmatu ajakirjaniku küsimustele, tasub tema taustaga tutvuda. Eriti kehtib see välisajakirjanike kohta. Mõned näpunäited:

- Otsi küsija nime Google'ist ja sotsiaalmeediast ning tutvu tema varasemate tööde ja tegemistega. Venekeelse ajakirjaniku puhul tee seda ka otsimootoris Yandex, kasutades kirillitsat. Kui keegi on mõne väljaande püsikirjutaja, siis on tema varasemad tööd üsna hõlpsasti leitavad. Lisaks hoiakutele ja stiilile annab see aimu, kas ta on konkreetset teemat varem katnud või mitte.
- Lisaks inimese enda taustale tutvu väljaandega, mida ta esindab. Kallutatud ja kontrollitud väljaanded võivad kasutada heausklikke neutraalseid ajakirjanikke, et enda legitiimsust tõsta.
- Vaata, mis aadressilt on inimene oma kirja saatnud. Kui ta kirjutab eraaadressilt ja väidab, et teeb vabakutselisena lugu mõnele tuntud väljaandele, siis võid talt julgelt küsida, kes ta toimetaja on.

NB! Kui asutuse poole pöördub Vene Föderatsiooni väljaande ajakirjanik, siis anna sellest enne vastamist teada riigikantselei strateegilise kommunikatsiooni meeskonnale aadressil stratkom@listid.rk.ee.

Allikakriitika veebis

Mida jälgida veebis uudiseid tarbides:

- Pealkiri: Pealkirja eesmärk on köita lugeja tähelepanu ning panna ta lugu avama. Loe alati pealkirjast kaugemale ning veendu, et pealkiri haakuks loo sisuga.
- Veebiaadress: Üks levinud taktika võltslehe autoriteedi suurendamiseks on mõne tuntud ja usaldusväärse lehe aadressi imiteerimine. Veendu, et veebilehe aadress haakuks selle sisuga.
- Sisu: Hinda loo sisu – kas see on informatiivne või arutlev? Kas see põhineb faktidel, emotsioonidel või arvamustel? Kui plaanid teksti oma tutvusringkonnaga jagada, siis loe see alati esmalt lõpuni.
- Õigekeel: Kuigi vigu teevad kõik, on usaldusväärsete väljaannete toimetused üldjuhul piisavalt professionaalsed, et mitte lubada sisse tõsiseid kirjavigu. Kui artikkel kubiseb kirjavigadest, on see taaskord üks ohumärk.
- Pildid: Pildimaterjal on üks viis tegelikkuse moonutamiseks. Pilte on lihtne töödelda – sellel olevaid detaile muuta, kustutada või neid sootuks lisada. Alati ei pea sedagi tegema, levinud on ka fotode eksitavas kontekstis kasutamine. Siin võib aidata tagurpidi pildiotsing (nt Google'i pildiotsing), mis näitab, kas pilti on varem teises kontekstis kasutatud.
- Autorlus: Ole tähelepanelik sisu osas, mille autorit pole välja toodud. Kui autor on välja toodud, siis mõtle, kes see on, ning kas tal võisid olla varjatud põhjused loo kirjutamiseks.
- Levik: Tõsiasi, et lugu on palju jagatud või kommenteeritud, ei ütle midagi selle sisu tõesuse kohta. Ära jaga materjali edasi pelgalt seetõttu, et paljud teised on seda enne sind teinud.