“Nähtamatu Paljastamise” töötoad

Informatsiooni rahvahankimine uurimuste läbiviimisel

Rahvahange: viitedokument

Sessioon 1: Sissejuhatus teemasse

Mis on rahvahankimine ja selle tekke lühike ajalugu:

- Termini rahvahankimine (*ingl k crowdsourcing)* tõi esimesena avalikkuse ette 2006. aastal ajakirja Wired artiklis Jeff How, kus ta defineeris seda kui uut viisi, kuidas internetist tööjõudu (all)hankida. Sealt edasi on välja kasvanud erinevat tüüpi kommertslikke ja mittekommertslikke rahvahankimisviise.
- Näites Wikipedia on parim näide kollektiivsest teadmiste hankimisest, KICK-STARTER on näide kaasrahastuse projektidest, Ushahidi on populaarne informatsiooni rahva-kaardistamise (ingl k *crowd-mapping)* platvorm.
- Seejuures nimetatakse Ushahidit üheks esimestest platvormidest, mis võimaldas “aktivistlikku kaardistamist” (*activist-mapping*) ehk aktivismi vormi, mis kombineerib rahvahankimise, kodanikuajakirjanduse ja georuumilise (*geospatial*) informatsiooni avaliku vastutuse ja sotsiaalse muutuse edendamiseks. Ushahidit kasutatakse sageli kriisiinformatsiooni rahva-kaardistamiseks.
- Ka ajakirjanikud kasutavad rahvahankimist üha sagedamini.

Rahvahankimise plussid ja miinused:

Plussid	Miinused
1. Võimaldab pääseda ligi suurele hulgale andmetele, mis muidu jääksid rahvahanke läbiviijale kättesaamatuks. 2. Võimaldab kaasata mitmekülgseid panustajaid. 3. Võib aidata säästa aega ja raha. 4. Avab uued võimalused koostöö tegemiseks kaasaaitajate ja/või teistega, kes töötavad samal alal.	1. Kaasneb manipulatsioonioht. 2. Võib vajada palju oskusteavet ja ressursse (nt tehniliste tööriistade ülesseadmine, kogutud andmete verifitseerimine jms). 3. Kaasneb tühjate pihkudega jäämise oht (rahvahankimise edu sõltub väga suuresti inimeste efektiivsest kaasahaaramisest). 4. Võivad kaasneda riskid korraldajatele ja panustajatele (nt kui rahvahangitakse sensitiivseid andmeid)

Manipulatsiooniriski maandamine:

- Arvestades rahvahangitud andmete verifitseerimise raskuse ja riskiga, et vastaspool "mürgitab" andmeid (nt bottide või pahatahtlike kasutajate abil), otsustavad paljud organisatsioonid kasutada rahvahankimist mitte esmase, vaid täiendava andmekogumismeetmena.
- Näiteks katastroofileevendamises ei ole haruldane kombineerida sotsiaalmeedias kasutajatelt saadud andmeid drooni- või satelliidifotodega.
- Valimiste vaatlemise ajal võivad valijate esitatud teateid rikkumiste kohta edasi uurida profesionaalsed valimisvaatlejad või ajakirjanikud ning selliseid teateid saab kasutada toetavate tõenditena protsessi ebakorrapärasuste kohta.

Võimalikud alternatiivid:

- Rahvahange vajab tihti palju *know-how'd* ja ressursse. Uurime seda edasi järgmises sektsioonis.
- Seetõttu võib mõnikord olla mõttekam kasutada teisi meetodeid, mis võivad anda samasugused tulemused - näiteks avalikel andmetel põhinev luure (ingl k *open source* intelligence ehk OSINT), mis keskendub tasuta tööriistadele ja ressurssidele.

Näited, kus rahvahanget võib kasutada ajakirjanduses, kriiside ajal, valitsemise parandamiseks, aruandluskohustuses või inimõiguste kaitsmisel:

Rahvahange ajakirjanduses

Columbia Graduate School of Journalismi Tow Center for Digital Journalism, mis uurib tehnoloogia mõju ajakirjanduses, peatus rahvahanke ajakirjanduses kasutamisel selles 2015. aasta juhises.

TOW defineerib ajakirjanduslikku rahvahanget kui "tegevust, mille käigus teadlikult kutsutakse gruppi inimesi osalema reporteritöös - nagu näiteks uudiste hankimine, andmete kogumine või analüüs. Seda tehakse sihitud ja avatud kutsega anda sisendit, jagada isiklikke kogemusi, dokumente või muud moodi panustama."

- 2018. aastal viis ABC Australia läbi riigi suurima rahvahankel põhinenud uurimuse, mis puudutas eakate hooldust.
- Saksamaa uuriva ajakirjanduse väljaanne CORRECTIV on välja töötanud efektiivse viisi, kuidas kaasata avalikkus andma rahvahangete kaudu informatsiooni. Nad teevad seda oma läbiproovitud CrowdNewsroom platvormi. Üks nende seni kõige edukamaid rahvahankel põhinevaid uurimusi oli "Kellele kuulub Hamburg?" (saadaval saksa keeles), mis kutsus Hamburgi elanikke üles läbi viima avalikku uurimust, kellele tegelikult kuuluvad ja kes kontrollib linna läbipaistmatul kinnisvaraturul rendikortereid.
- Bellingcat on veebipõhistele kodanikuuurimustele keskendunud organisatsioon, mis kasutab oma lugude ja artiklite osana tihti sotsiaalmeedia rahvahanget, et koguda informatsiooni, dokumente ja verifitseerida sündmusi. Üks nende tuntumaid

uurimusi on Malaysian Airlinesi lennu MH17 allatulistamisest 2014. aastal Ukrainas. See põhines suures osas rahvahankel.

- Mehhiko narkosõdade tõttu kannatada saanud perekondadest rääkinud dokumentaalfilmi "Anyone's Child Mexico" autorid kogusid lugusid läbi kohalike organisatsioonide tasuta telefoniliinide, paludes inimestel üle riigi helistada ja rääkida oma lugu.

Rahvahankimine kriiside kaardistamiseks

Ushahidi platvormi kasutamist 2010. aasta Haiti maavärina ajal peetakse esimeseks näiteks rahvahanke kasutamisest katastroofimõjude leevendamisel. Sellest ajast saati on arendatud mitmeid teisigi rahva-kaardistamise platvorme ning neid on kasutatud humanitaarkriisides, sealhulgas kombineerituna muude tehnoloogiatega nagu näiteks drooni- ja satelliidifotod.

- Siin on näide 2021. aastast, kui rahvahanke abil kaardistati Indoneesias kätepesujaamad, et tõkestada COVID-19 levikut.

Rahvahankimine paremaks valitsemiseks, aruandluse kohustuse parandamiseks ja inimõiguste kaitseks

Aktivistid ja inimõiguste kaitsjad on kasutanud rahvahanget ka altkäemaksude ja korruptsiooni kaardistamiseks, inimeste aitamiseks võimudele kohalikest probleemidest teatamisel ja inimõiguste rikkumise paljastamiseks.

- Siin on näide 2017. aastast Amnesty Internationali ja Airwarsi ühisest uurimusest Süüria linna Raqqa pommitamise kohta, mis sisaldas rohkem kui 138 000 vabatahtliku panustamist 124 riigist.
- ProPublica on sõltumatu mittetulunduslik väljaanne, mis tegeleb uuriva ajakirjandusega. 2020. aastal korraldas ta USA valimispäeva kollaboratiivse reaalajas kajastuse - nimega ElectionLand - mille käigus rahvahangiti valijatelt andmeid läbi veebivormistike, tekstisõnumite ja WhatsAppi.

Sessioon 2: rahvahanke ülesseadmine

Enne rahvahankega alustamist on oluline küsida mitmeid küsimusi. Küsimused, mille alusel pidada arutelu, on järgmised:

- **Miks sa tahad rahvahankida?**
  - Näiteks: et rääkida lugu / tõsta teadlikkust mõne probleemi kohta; koguda andmeid, et aidata teisi aktiviste või organisatsioone nende tööga; kaasata kodanikke olulise protsessi või sündmuse juurde või muu. Näiteks:

        - Suur online-petitsioon, mis nõuab koroonavaktsiini ülemaailmset kättesaadavust
        - Reaalajas ülemaailmne õhukvaliteedi kaart
        - Platvorm, mida inimesed saavad kasutada kohalikele võimudele probleemidest teatamiseks

- **Millised on peamised eetilised kaalutlused, kui rahvahankida tõendeid?**
    - Võid soovida kaaluda selliseid aspekte nagu informatsiooni täpsus, panustajate privaatsus, kogutud andmete omandiküsimus või sinu tegevuse kättesaadavus.
    - Mõnede nende aspektidega võivad kaasneda ka juriidilised kaalutlused. Seega võib olla tark mõte konsulteerida enne rahvahanke korraldamist juristidega.

- **Kui verifitseeritavad kogutud andmed on?**
    - Rahvahankimine võib olla kasulik tööriist, et koguda andmeid, mida sa ei pruugi teada.
    - Ent nende andmete verifitseerimine võib osutuda raskeks, eriti kui sinu vastas seisab suurem osapool, kes saab käiku lasta nii botid kui inimesed, et sinu andmeid korrupteerida. Seega on enne rahvahankega alustamist mõistlik hoolikalt kaaluda, kas ja kuidas on kogutavad andmed kontrollitavad.
    - Selgita välja, millises ulatuses suudad sa andmeid enne nende avaldamist verifitseerida. Kui sul on viiteid, et andmeid võib olla taotluslikult korrupteeritud, kaalu hoolikalt, kas neid peaks üldse avaldama. Näiteks:
        - Venemaa valimisrikkumiste rahva-kaardistamise platvorm https://www.karta-narusheniy.org/ esitab lahtiütluse, mille kohaselt esitavad teavet valimisrikkumiste kohta kasutajad vabatahtlikult ning seda teavet enne avaldamist eraldi ei verifitseerita, sest eesmärk on see teha võimalikult kiiresti nähtavaks valimiskomisjonidele ja õiguskaitseasutustele (sisu on vene keeles).

- **Kes on sinu kaasaaitajad, panustajad?**
    - Väljaõppinud aktivistidelt panustamise küsimine võib olla hoopis erinev kui tavakodanike kaasamine.
    - Võid tahta kaaluda ka selliseid demograafilisi iseärasuseid nagu vanus, sugu või panustajate geograafiline asukoht.
    - Kui sa ei soovi, et kogutavad andmed pärineksid vaid ühelt elanikkonna segmendilt, küsi enda käest, kas su püüded saavad jõuda ka marginaalsemate gruppideni ning kas kasutatavad tööriistad on võrdselt kättesaadavad kõigile või võivad need suurendada olemasolevaid digitaalseid lõhesid.
    - Viimaseks, ehkki andmed ei pruugi olla representatiivsed sotsioloogilises mõttes, võid siiski soovida, et need pärineksid eri asupaikadest ja erinevatest ühiskonnagruppidest, et saada olukorrast ette võimalikult täpse pildi.

- **Kes on sinu kasusaajad?**
    - Pea meeles, et need, kes panustavad su rahvahankesse andmetega ja sinu töö lõplikud kasusaajad võivad erineda.

- Proovi esitada oma tulemused formaadis, mis on sinu auditooriumile, kellega soovid seda jagada, kättesaadav. See võib mõjutada ka seda, millises formaadis soovid andmeid rahvahankida. Näiteks:
  - Veebileht "I Paid a Bribe" - projekt, mis träkkis korruptsiooni Indias - näitab riigikaarti vastavalt igast regioonist pärinevate teadaannete arvule, avaldab üksikraporteid reaalajas, liidab need kategooriate kaudu kokku ja annab ülevaate kaasnevast uudiskajastusest.

- **Mis on riskid?**
  - Oluline on mõelda ka riskidest või turvalisuskaalutlustest, mis võivad mõjutada sind või rahvahankesse panustajaid. Samuti mõtle, kas nad on neist riskidest teadlikud.
  - Tee kõik mis võimalik, et vajadusel kaitsta nende privaatsust ja anonüümsust. Teinekord võib see tähendada lisasammude astumist, et andmed enne edasist töötlemist deanonümiseerida.

- **Kas sina hakkaksid enda partneriks või kaastöötajaks?**
  - Mõtle teiste gruppide või aktivistide peale, kes võiksid olla sinu tööst huvitatud või juba tegeleda samalaadse tööga. Kas on olemas gruppe, kellel on andmete rahvahankimise kogemus või kelle andmeid sa saad kasutada oma tulemustega ristvõrdlemiseks?
  - Tavaliselt on teistega partnerlusse asumine hea mõte ning aitab parandada oma töö tulemust või vältida kordamist.
  - Lisaks võib koostöö tulemusel tekkida lõbusaid ühendatud andmekogusid. Näiteks:
    - ProPublica Electionland kujutas endast kollaboratiivse ajakirjanduse projekti, mis kajastas valimistest osavõtmise võimalusi, küberturvalisust, desinformatsiooni ja valimiste aususe teemasid USA 2020. aasta valimistel. Selleks, et kajastada valimistega seotud ebakorrapärasusi reaalajas, kaasas ProPublica üle 150 meediaväljaande üle riigi ning kutsus üles valijaid, küsitlustetegijaid ja valimiskomisjonide liikmeid, et nood annaksid eri kanalite kaudu teada kõikvõimalikest probleemidest, mida nad valimisprotsessi kestel kogevad.

- **Mis saab andmetest pärastpoole?**
  - Näiteks kas sa soovid avalikult jagada toorandmeid või kirjutada tulemuste põhjal kokku raporti ja levitada seda?
  - Kas on kriitiliselt oluline avaldada tulemused otsekohe?
  - Millises formaadis peavad andmed olema? Näiteks:
    - FixMyStreet avaldab Ühendkuningriikides reaalajas ekraanil koondandmeid kodanike poolt raporteeritud probleemidest ning reastab probleemide peamised kategooriad, jälgib, kui palju probleeme on juba lahendatud ja annab omavalitsustele hindeid vastavalt nende valmidusele probleemidele reageerida.

- **Kas kedagi tuleb tunnustada autorina või allikana ja kuidas seda teha?**
  - Kui keegi seda väärib, on alaline oluline neid tunnustada.
  - See võib tähendada koostööd teinud organisatsioonide tänamist, kasutatud tööriistade ja tarkvara väljatoomist ja isegi panustajate nimepidi nimetamist (grupid või kõige aktiivsemad üksikisikud eriti suurtes projektides), kui nad ei soovi jääda anonüümseks.
  - Küsi alati panustajatelt üle, kuidas nad soovivad nimetatud saada või lisa selle kohta märge juba eelnevalt, tuues ka välja, kuidas võib sellisest viitamisest loobuda, kui see kujutab neile mingeid riske. Näiteks:
    - Kui Amnesty International ja Airwars avaldasid uurimuse Süürias Raqqa linnas 2017. aastal pommitamise käigus hukkunud tsiviilisikutest, tõid nad välja kõik partnerid, tööriistad ja peamised panustajad, kes aitasid koguda erinevaid tõendeid (vaata https://raqqa.amnesty.org/ => “Toolkit” => “Credits”).

Sessioon 3: õige rahvahankimise lähenemise valimine

Õige lähenemise valimine sõltub sinu eesmärkidest.

Mõnikord panevad ajakirjanikud püsti turvalise kanali, kus inimesed saavad anonüümselt saata vihjeid; inimõiguste kaitsjad võivad julgustada ohvreid esitama väärkohtlemise tõendeid ükskõik mis formaadis need neil olemas on; valimisvaatlejad võivad tahta, et valijad prooviksid nähtud ebakorrapärasust kategoriseerida etteantud kriteeriumite alusel.

Sõltuvalt sellest, kui palju sul on tarvis, et rahvahangitud andmed oleksid kindlale analüüsile sobivas formaadis, saad otsustada, kas pead koguma struktureeritud või struktureerimata andmeid.

- Columbia Ülikooli Tow Center for Digital Journalismi koostatud rahvahankimise juhend eristab **“avatud” ja “spetsiifilisi” üleskutseid**:
  - ”Avatud” üleskutsetes kutsutakse avalikkust ajakirjanikega avatult ühendust võtma läbi erinevate kanalite (e-post, telefon, SMS, veebiküsitluse tarkvara jne), et panustada hääletamisega, vihjetega, kõnedega või mistahes muu materjaliga, mida nad soovivad uudisteväljaandele / ajakirjanikule edastada. See formaat kätkeb tavaliselt endas avatud andmete kogumist.
  - “Spetsiifilises” üleskutses sihib ajakirjanik kindlaid gruppe spetsiifilise info jagamise palvega. Sellist informatsiooni edastatakse tavaliselt eelnevalt määratud formaadis, mida kogutakse otsitavasse andmebaasi.

- **Spetsiifiliste andmete struktureeritud viisil rahvahankimise eelised** sisaldavad kindlat tüüpi tõendite kogumist ühtsesse formaati, mis lubab andmeid kergemalt analüüsida. Kuid rangem formaat võib piirata sihtauditooriumi võimekust andmeid edastada.

- Avatud ja **struktureerimata üleskutsed** võivad rahvahankida laiemat laadi andmeid potentsiaalselt rohkematelt panustajatelt ilma ennast ja oma auditooriumi piiramata kindlate raamidega, milliseid andmeid sa eeldad saavat. Samal ajal võib erinevatest kanalitest erinevates formaatides tulevate andmete verifitseerimine ja analüüsimine olla palju töö- ja ajamahukam.

- Mõnikord võib kasutada **segalähenemist**, seda eriti suurtes kollaboratiivsetes projektides või kui andmeid tuleb ristkontrollida erinevate tõendivoogude vahel.

Sessioon 4: Rahvahanke sihtauditooriumiga töötamine

Kogukonna edukas kaasamine, kellelt sa andmetega panustamist saada soovid, on pool rahvahankimise õnnestumisest.

Teiste sõnadega: võid teha kõik muu õigesti, aga kui mitte keegi andmetega ei panusta, on kogu su töö tulutu. Seetõttu on kriitiliselt oluline mõelda kogukonna kaasamisele juba varakult.

- Siin on mõned **abistavad küsimused** ProPublicalt:
  - Kes on need inimesed, keda sa tahad, et vastaksid? Miks on just nemad parim kogukond, keda kaasata?
  - Mida see kogukond sellest võidab? Millistel põhjustel peaks keegi osalema?
  - Millised on põhjused, miks mõned ei pruugi soovida osaleda? Kuidas sa kavatsed leevendada nende kahtlusi ja muresid?
  - Keda see kõige rohkem mõjutab? Mis keelt nad kasutavad, et probleemi kirjeldada? Kas nad on vihased? Kus nad sellest räägivad? Kuidas?
  - Kes on selles kogukonnas kõige mõjukamad inimesed? Kas sa oled nendega rääkinud? Mida nad sinu mõttest arvavad?

- Kindlasti mõtle läbi ka see, millistes **spetsiifilistes sotsiaalsetes ja poliitilistes tingimustes** sa tegutsed.
  - Kui sulle andmete edastamine tähendab teatavat riskitaset, on inimesed kõhkleval seisukohal ning neil oleks vaja uskuda, et sellest võib välja kasvada nähtav muutus.

- Mõtle, **kuidas saad panna inimesed huvi tundma ja õhinasse minema** võimalusest olla su rahvahanke protsessis osaline.
  - Mõnikord võib see tähendada, et rahvahankele peaks eelnema teadlikkuse tõstmise või usalduse tekitamise töö.

- Võid läbi viia konkreetse probleemi kohta infokampaania, kaasata arvamusliidrid, rajada usaldusliku suhte kogukonna kõige aktiivsemate liikmetega jne.

- Mõtle, **kuidas sa näitad tulemusi** ja tagasisidestad oma auditooriumi isegi siis, kui panustajad jäävad anonüümseks. Näiteks:
  - võid avaldada rahvahankimise kulgemisest reaalajas uuendusi või isegi jagada osa kogutud andmetest samu kanaleid pidi, et julgustada rohkemaid inimesi panustama (vaata "Anyone's Child: Mexico" kaasust, mis on selle ideaalne näide).
  - Samuti aitab, kui mõned abipanused saabuvad nii kiiresti kui võimalik pärast rahvahanke käivitamist (seda saab eelnevalt korraldada mõne usaldusväärse allikaga, kui sa tead, et neil on juba, millega panustada).
  - **Lühidalt, kui kogukonna liikmed näevad, et teised osalevad aktiivselt, tulevad ka nemad sellega suurema tõenäosusega kaasa.**

- Mõtle, **kuidas sa kavatsed jõuda oma auditooriumini**.
  - Võid tahta oma üleskutseid edastada kanalites ja meetoditega, mida eelistab sinu sihtauditoorium ja mitte tingimata sina ise.
  - Näiteks sihitud veebireklaamitööriistad nagu Facebooki Lookalike Audiences võivad olla väga võimsad, aga vaid siis, kui su sihtauditoorium üldse kasutab Facebooki ja kui sul on piisavalt raha, et kulutada seda Facebooki reklaamidele.
  - ProPublica pakub **mitmeid abistavaid küsimusi**, mille peale mõelda, kui valid õiget kaasamismeetodit:
    - Milline on parim ja kõige efektiivsem suhtlemisvorm selle kogukonnaga? Kuidas annad osalejatele teada, mida sa leiad? Kui kaasatud sa tahad/vajad, et see kogukond kogu uurimistöö jooksul oleks?
    - Mida sa tahad, et inimesed sulle kaasamise ajal räägiksid? Kas sa tahad rahvahankida andmeid, lugude/jutustuste kogumit, koguda tõendusmaterjali vms?
    - Milliseid konkreetseid informatsiooni tükke sa vajad? Milline on osaleja jaoks lihtsaim viis, et seda sulle anda? Kas sa oled teinud kasutaja-testi? Mis juhtus?
    - Kui projekt levib plahvatuslikult ja saad hiiglaslikult vastuseid, kuidas sa need organiseerid? Mis süsteemid vms pead sa enne valmis seadma?
    - Kuidas sa kasutad või avaldad seda infot, mida osalejad sulle saadavad? Millised õigused nad sulle annavad? Milline on parim ja selgeim viis, kuidas oma kavatsusi neile kommunikeerida?
  - Siin on mõningad **kogukonna poole pöördumise meetodid ja kanalid,** mida võid kaaluda: (rohkem leiad Global Investigative Journalism Networki tsiteeritud juhtumiuuringutest.):
    - Hollandi väljaande *De Correspondent* reporter Jelmer Mommers kasutas väljaande veebilehte, et pöörduda otse Shelli töötajate poole, et saada neilt informatsiooni ettevõtte teadmiste kohta kliimamuutusest. Ta kutsus lugejaid talle e-kirju saatma ja sai ettevõtte sisedokumente ja muudki.
    - USA *ProPublica* kaasamise reporter Adriana Gallardo tegi koostööd National Public Radio korrespondendi Renee Montagne'iga, et levitada sünnitusel elu-

ohtlikke komplikatsioone kogenud naistele suunatud veebiküsimustikku. See avaldati Facebookis ja Twitteris ning ebakonventsionaalsetes kanalites nagu näiteks kaasrahastuse platvormil GoFundMe ning küsimustele vastati tuhandeid kordi, mille abil avaldas ajakirjanik mitmeid lugusid.

- Mehhiko narkovägivallast dokumentaalfilmi vändanud filmitegijad käivitasid tasuta telefoniliini ning reklaamisid seda kohalike partnerite abil ning kutsusid üle riigi inimesi üles helistama ja rääkima oma lugusid. Kui nad helistasid, võisid osalejad kuulata ka teiste helistanute lugusid. See rahvahange päädis multimeedia dokumentaalprojektiga "Anyone's Child: Mexico" (saadaval ka hispaania keeles).

- Kindlasti võta arvesse kõiki **privaatsuse ja turavalisuse** kaalutlusi.
  - Kas sinu rahvahanke projektis osalemine võib su sihtauditooriumile kaasa tuua mingeid riske? Kui jah, on kriitiliselt oluline, et sa teed kõik, mis on sinu võimuses, et käivitada turvaline kommunikatsioonikanal ja kaitsta panustajate identiteete.
  - Kuigi inimesed võivad oma turvalisuse osas olla leplikumad kui sa eeldad, pead püüdma kindlustada, et nad saaksid aru riskidest ja sellest, kui palju on sinul võimalik neid riske maandada.

Sessioon 5: Rahvahankimiseks tehniliste tööriistade valimine

Võib lihtsasti ülemääraselt erutuda mõnest kindlast tehnilisest tööriistast, mille abil rahvahange korraldada. Saadaval on rohkelt lihtsalt kasutatavaid ja turvalisi tööriistasid, mille on arendanud inimõiguste kaitsjad, ajakirjanikud või kolmanda sektori järelevalveorganisatsioonid. Sellegipoolest on oluline valida õige tööriist, mis sobib kõige paremini kokku just sinu rahvahanke eesmärkide ja vajadustega, mitte proovida kujundada rahvahanget ühe konkreetse tööriista järgi. Mõnikord tähendab see, et sul ei lähe vaja kõige uuemat ja ägedamat tehnoloogiat, vaid võid selle asemel valida lihtsa telefoni kõneliini, tekstisõnumite saatmise või e-maili.

Parima valiku tegemiseks tuleb kaaluda:

- **Tehniline keskkond**
  - Kas enamusel sihtauditooriumi liikmetest on ligipääs internetile? Milline ühendus neil on?
  - Kas neil on ligipääs mobiillseadmetele või nutitelefonidele ja kui nii, milliseid vahendeid/mudeleid nad tõenäoliselt kasutavad?
  - Mõtle ka nende arvutioskuse peale.

- **Privaatsus ja turvalisus**
  - Oluline on kaaluda, kas sinu rahvahankes osalemine võib sihtauditooriumile kaasa tuua riske. Kui jah, on kriitiliselt oluline, et sa teed kõik, mis on sinu võimuses, et käivitada turvaline kommunikatsioonikanal ja kaitsta panustajate identiteete.

- Kuigi inimesed võivad oma turvalisuse osas olla leplikumad kui sa eeldad, pead püüdma kindlustada, et nad saaksid aru riskidest ja sellest, kui palju on sinul võimalik neid riske maandada.

- **Olemasolevate tööriistade kasutamine või millegi uue ehitamine / kasutusele võtmine**
  - Inimesed on just oma tehnoloogiaharjumuste muutmise osas vastumeelsed. Uuri, milliseid tehnikatööriistu sinu sihtauditoorium juba kasutab (nt sotsiaalmeedia, online-suhtlusrakendused jne) ja kaalu nende tööriistade integreerimist oma rahvahankesse.
  - Kui otsustad rahvahankeks arendada ja kasutusele võtta spetsiaalse uue tööriista, arvesta, et hoolimata sinu parimatest püüetest panna inimesed seda kasutama, võib see võtta palju aega või üldsegi mitte õnnestuda.

- **Mõned populaarsed ja turvalised kommunikatsioonitööriistad ning nende plussid ja miinused**
  - Ajakirjanikud ja aktivistid kasutavad mitmeid turvalisi suhtluskanaleid. Ehkki mitte ükski süsteem ei ole 100% turvaline, püüavad mõned tööriistad luua turvalisemat keskkonda kui tavapärased suhtluskanalid (nagu telefon, sotsiaalmeedia, e-mail).
  - Mitte üksksi tööriist ei ole kõige parem absoluutselt kõigi jaoks, seega on oluline hoolikalt kaaluda sinu perspektiivsete panustajate individuaalseid asjaolusid.

Tavapäraste kommunikatsioonikanalite seas on:

Tööriistad	**Eripärad**	**Miinused**	**Allalaadimine ja seadistamise juhised**
Signal https://signal.org/	Signal on tasuta ja vabavaraline turvaline suhtlusrakendus iPhone'i ja Androidi seadmetele, mida arendab Open Whisper Systems. See krüpteerib kogu kommunikatsiooni otsast otsani, tehes kogu kommunikatsiooni kättesaadavaks ainult saatjale ja vastuvõtjale.	Signal ei ole ligilähedaseltki nii populaarne nagu WhatsApp või teised otsast otsani krüpteeritud suhtlusrakendused ning kasutajad peavad registreerima oma tegelike telefoninumbritega. Sellegipoolest, ei salvesta Signal sisuliselt mitte üldse sinu kontaktide või sõnumite metaandmeid, tehes rakenduse kasutamise andmete pealt sinu kommunikatsioonist millegi teada saamise võimatuks.	https://signal.org/download/

WhatsApp https://www.whatsapp.com/	Saadaval iPhone'il ja Androidis. WhatsApp on populaarne suhtlusrakendus, mis kasutab Signaliga sarnast otsast otsani krüpteeringut. Seda kasutab praegu üle maailma rohkem kui 2 miljardit inimest.	Nagu Signal, salvestab WhatsApp kasutaja telefoninumbri. See kuulub Facebookile ning kasutaja telefoninumbrit ja analüütikat jagatakse sotsiaalmeediafirmaga. Facebook võib olla sunnitud oma rikkalikke kasutajaandmeid jagama kohtuorderite alusel. WhatsApp võib ka varundada su krüpteeritud sõnumid iCloudis või Google Drive'is, ent seda võimalust saab rakenduse turvalisusesätingutest maha keerata.	https://www.whatsapp.com/download/
Pretty Good Privacy (PGP) emaili krüpteerimine	PGP on krüpteerimisstandard, mis on ajakirjanike seas populaarne emailide kaitsmiseks. See kasutab avaliku võtme krüptograafiat, mis tähendab, et igal kasutajal on "avalik võti", mida kasutatakse teistele kasutajatele saadetavate sõnumite krüpteerimiseks. Avalikku võtit võib jagada kõigiga. Igal kasutajal on ka vastav "privaatne võti", mida kasutatakse sõnumite kokkupanemiseks ja mida ei tohi mitte kunagi jagada. Emailide krüpteerimise tarkvara näited on GPG Suite Maci jaoks, GPG4win Windowsile ja Linuxile, Thunderbird koos Enigmaili laiendusega, ja Mailvelope.	PGP vajab teataval tasemel tehnilisi teadmisi ja väljaõpet, enne kui tavaline arvuti- ja nutitelefonikasutaja seda kasutada saab. Teised turvalise kommunikatsiooni kanalid võivad pakkuda samalaadset kaitsetaset, aga olla kasutajasõbralikumad.	https://www.openpgp.org/software/
Protonmail https://proton.me/	ProtonMail on PGP-ga täielikult integreeritud tasuta emailiteenus. See tähendab, et ProtonMailiga saab igaüks kasutada PGP-d sõltumata oma tehnilistest teadmistest. See ei lase ka mitte kellelgi, sealhulgas ProtonMailil endal, sinu	Ehkki tasuta (basic konto ainult) ja lihtne kasutada, suhtleb ProtonMail väliste emaili-kontodega vaikimisi ilma otsast otsani krüpteeringuta. Seega võib välisel e-maili teenuse pakkujal olla ligipääs ProtonMailiga	https://proton.me/pricing

	emaile lugeda või neid jagada. Seda kontseptsiooni teatakse kui null-ligipääsu krüpteeringut.	saadetud sõnumitele. See tähendab, et tundlikku informatsiooni on mõistlik edastada ainult ProtonMaili teenuse sees.	
SecureDrop https://securedrop.org	SecureDrop on vabavaraline vilepuhumise süsteem, mille ajakirjandusorganisatsioonid saavad endale üles seada, et vilepuhujatel ja allikatel oleks võimalik turvaliselt ja anonüümselt saata dokumente ja vihjeid. See on saadaval 20 erinevas keeles ja seda kasutab üle 50 meediakanali üle maailma, teise seas *The New York Times, The Washington Post*, *ProPublica*, *The Globe and Mail* ja *The Intercept.*	Samas kui SecureDrop lubab seda endale ülesseadvatel organisatsioonidel hoida kogu info enda serverites, minimeerib metadata, krüpteerib andmed ja kasutab rida muid tugevaid turvameetmeid, võib selle ise püstipanemine olla kulukas ja keeruline.	https://docs.securedrop.org/en/stable/
Tella https://tella-app.org/	Tella on tasuta vabavaraline mobiillse andmeside rakendus, mis on mõeldud piiratud internetiühendusega ja suurte turvalisusriskidega piirkondade jaoks. Hetkel on see saadaval Androidil ning paljudes eri keeltes.	Ehkki Tellat on võrdlemisi lihtne kasutada ja seda saab mugandada organisatsiooni vajaduste järgi, vajab rakenduse kasutamine siiski koolitust ja serveri ülesseadmiseks tehnilisi oskuseid.	https://tella-app.org/
FrontlineSMS https://www.frontlinesms.com	Erinevate organisatsioonide poolt kasutatud tarkvara, mis levitab ja kogub tekstisõnumite abil informatsiooni enam kui 120 riigis.	Kasutab üldkättesaadavat ent ebaturvalist kommunikatsioonikanalit. Tasuline, ent võrdlemisi madalate tasudega teenus.	https://www.frontlinesms.com/platform

Sessiion 6: Verifikatsioon

Rahvahangitud andmete verifitseerimine on ülioluline. Mõtle hoolikalt, kui palju verifitseerimist sa tahaksid ja suudaksid läbi viia arvestades kogutavate andmete tüüpi ja formaati.

Tulemused võivad välja näha nii:

- **Verifitseerimata andmed**
  - Osasid andmeid ei pruugi olla võimalik kontrollida, sest need võivad olla uued ning kinnitavaid allikaid napib. Sel juhul mõtle verifitseerimise asemel kontrollimisele (ingl keeles *vetting*). See tähendab katset andmeid enne avaldamist ümber lükata.
  - **Kui sa ei suuda andmeid verifitseerida, aga tahad neid ikkagi avalikustada, lisa nende juurde selge diskleimer, mis märgistab, et andmed on verifitseerimata.**

- **Osaliselt verifitseeritud andmed**
  - Otsusta, kui paljust verifitseerimisest piisab, et andmeid saaks kasutada / avaldada

- **Täielikult verifitseeritud andmed**
  - Tavaliselt andmed, mida kinnitavad mitmed täiendavad allikad.
    - Kui kajastad reaalajas (inim)õiguste rikkumisi või kui toimunu tuleb avalikustada kiiresti, et takistada pahategude toimepanemist või edasise kahju tekkimist, kaalu “põllule” mobiilse ja kvalifitseeritud meeskonna saatmist, kes saaks sündmuspaika külastada ja koguda kinnitavaid tõendeid;
    - Kui kohapealne verifitseerimine ei ole võimalik, võivad korraldajad otsustada teha koostööd kellegagi, kellel on kohapeal jõud olemas ning kellega saab tulemusi ristvõrrelda.

Rahvakaardistatud andmete verifitseerimine

Kriisi ajal informatsiooni rahvahankimisel tuleb arvestada mitmete asjaoludega. Ushahidi kasutajad tuvastasid Haiti 2010. aasta maavärina ajal järgmised andmete verifitseerimise viisid, sealhulgas kui andmed on joonistatud kaardile:

- **asukoht** – kas sisend tuleb õigest asukohast?
- **reputatsioon** – kas allikat usaldad sina või usaldavad usaldusväärsed inimesed?
- **sisu võrdlus / koondamine** – klasterdamise või teiste meetodite kaudu mustrite leidmine
- **ajastus** – kas sisend tuleb õigel ajal?

Sotsiaalmeedias informatsiooni verifitseerimine

Kui sa kogud just sellist tüüpi andmeid nagu sotsiaalmeedia postitused, multimeedia failid jne, saab neid verifitseerida mitmete tehnikate abil (vaata nt European Journalism Centre’’i Sotsiaalmeedia verifitseerimise käsiraamat). Pead siiski meeles pidama, et verifitseerimis-

protsessi ülesseadmine ei ole lihtne ülesanne ning see võib vajada keerulist otsustuspuu mudelit ja spetsiifiliste oskustega meeskonda.

- Vaata seda näidet, kuidas ajakirjanikud püüdsid monitoorida ja verifitseerida Ukraina 2012. aasta parlamendivalimistega seotud informatsiooni.

Sessioon 7: Andmete analüüsimine ja tulemuste esitamine

Oluline on rahvahangitud andmed avaldada ausal ja tõesel viisil, aga samuti tuleb mõelda haaravale formaadile, kuidas seda esitada.

- Enne rahvahankega alustamist, mõtle, kuidas sa tulemusi **analüüsid** ja **esitad**. **Formaat,** milles sa võib soovida tulemused avaldada, võib mõjutada formaati, milles sa andmeid rahvahangid.
  - Näiteks, kui sa soovid kirjutada loo või artiklisarja, mis põhineb kogutud andmetel, võib kõige sobilikum olla kasutada struktureerimata rahvahanke vormi. Kui aga, vastupidi, soovid kirjutada analüütilise raporti, võid vajada rohkem struktureeritud andmeid, mida saab süsteemsemalt analüüsida.
  - Isegi kui sa töötad struktureeritud andmetega, mõtle, millist muljet sa oma andmetega soovid jätta; teiste sõnadega, millist lugu sa tahaksid oma andmetega rääkida?

- Tulemuste avaldamisel **kirjelda** nii andmete kogumise **meetodeid** kui ka seda, **kuidas** sa järeldusteni jõudsid (juhul kui viisid läbi analüüsi).

- Ära unusta **tunnustamast teisi** alati, kui nad seda väärivad. See võib sisaldada koostööd teinud organisatsioonide tänamist, kasutatud tööriistade ja tarkvara väljatoomist ning isegi panustajate (gruppide või kõige aktiivsemate üksikisikute) nimepidi nimetamist - ent mitte juhul, kui nad soovivad jääda anonüümseks.
- Too selgelt välja nii oma veebilehel kui ükskõik millises muus materjalis, mida sa oma tulemuste põhjal avaldad, kas ja millises ulatuses suutsid sa rahvahangitud andmed **verifitseerida**.

Seotud vahendid: “Nähtamatu Paljastamise” artiklid ja juhised

- “Läheb vaja rahvast...”: Rahahankega informatsiooni kogumise vihjed ja näited”, artikkel, millega kaasneb “Nähtamatu Paljastamise” konverentsi videokõne ja juhtumiuuringu videoesitlus
- "Ohutus ennekõike!", “Nähtamatu Paljastamine: varustus” juhend.
- "Riskihindamine on mõtteviis mitte kontrollnimekiri", artikkel, millega kaasneb “Nähtamatu Paljastamise” konverentsi videokõne.