“Exposing the Invisible” Mokymai

Sutelktinio informacijos rinkimo (crowdsourcing) informacija tyrimams

Crowdsourcing: Informacinis dokumentas

1 sesija: įvadas į temą

Kas yra „crowdsourcing“ ir trumpa jo atsiradimo istorija:

- Sąvoką „crowdsourcing“ pirmasis įvedė Jeffas Howas 2006 m. žurnalo „Wired“ straipsnyje, kuriame jis tai apibrėžė kaip naują darbo jėgos apsirūpinimo būdą, kurį įgalina internetas. Nuo to laiko atsirado įvairių komercinių ir nekomercinių „crowdsourcing“ apraiškų.
- Pavyzdžiui, Wikipedia yra geriausias „crowdsourcing“ pavyzdys KICKSTARTER yra sutelktinio finansavimo projektų pavyzdys, Ushahidi yra populiari minios žemėlapių informacijos platforma.
- Tiesą sakant, Ushahidi buvo giriama už tai, kad tapo viena pirmųjų platformų, kuri įgalino “activist mapping,” arba tam tikros rūšies aktyvizmą, kuris sujungia „crowdsourcing“, piliečių žurnalistiką ir geo erdvinę informaciją socialiniams pokyčiams ar viešajai atskaitomybei. Dažniausiai Ushahidi buvo naudojamas krizių informacijai nustatyti.
- Sutelktinis informacijos gavimo būdas išpopuliarėjo ir yra naudojamas žurnalistų.

„Crowdsourcing“ privalumai ir trūkumai:

Privalumai	Trūkumai
1. Leidžia pasiekti didžiulį duomenų telkinį, kuris kitu atveju organizatoriams nepasiekiamas. 2. Leidžia įtraukti įvairius bendraminčius. 3. Gali padėti sutaupyti laiko ir išlaidų. 4. Atveria naujas galimybes bendradarbiauti su bendradarbiais ir (arba) kitais, dirbančiais toje pačioje erdvėje.	1. Kyla manipuliavimo pavojus. 2. Gali prireikti daug žinių ir. išteklių (pvz., techniniams įrankiams nustatyti, surinktiems duomenims tikrinti ir kt.). 3. Kyla pavojus likti tuščiomis rankomis (sėkmė labai priklauso nuo efektyvaus bendradarbių įtraukimo). 4. Gali sukelti pavojų organizatoriams. ir bendraautoriams (pvz., kai surenkami slapti duomenys)

Manipuliavimo rizikos suvaldymas:

- Atsižvelgę į iššūkius, kylančius tikrinant duomenis, ir riziką, kad duomenis sugadins priešiški subjektai (pvz., dėl robotų ar piktybinių naudotojų pastangų), daugelis organizacijų pasirinko „crowdsourcing“ naudoti ne kaip pagrindinį, o kaip papildomą duomenų rinkimo metodą.
- Pavyzdžiui, teikiant pagalbą nelaimės atveju, socialinių tinklų naudotojų sugeneruoti duomenys neretai derinami su dronų filmuota medžiaga ar palydoviniais vaizdais.
- Stebint rinkimus, rinkėjų pranešimus gali toliau tirti profesionalūs rinkimų stebėtojai arba žurnalistai ir jie gali būti kaip proceso pažeidimų įrodymas.

Galimos alternatyvos:

- „Crowdsourcing“ dažnai reikalauja daug žinių ir išteklių, kurie bus toliau nagrinėjami kitame skyriuje.
- Todėl kartais labiau įmanoma naudoti kitus metodus, galinčius duoti panašių rezultatų, pavyzdžiui, atvirojo kodo žvalgybos (OSINT), kurios pagrindinis dėmesys skiriamas nemokamų įrankių ir išteklių naudojimui.

Pavyzdžiai, kada žurnalistai gali pasinaudoti „crowdsourcing“ krizės metu arba siekdami geresnio valdymo, atskaitomybės ar žmogaus teisių gynimo:

Sutelktinis informacijos paieškos mechanizmas („crowdsourcing“) žurnalistikoje

Kolumbijos aukštosios žurnalistikos mokyklos skaitmeninės žurnalistikos centras „Tow Center for Graduate School of Journalism“, kuris tiria technologijų poveikį žurnalistikai, tiria, kaip žiniasklaida gali naudoti minios šaltinį 2015 guide.

Žurnalistikoje TOW apibrėžia minios šaltinį kaip „konkretų žmonių grupės pakvietimą dalyvauti ataskaitų teikimo užduotyje – pavyzdžiui, renkant naujienas, renkant duomenis ar analizuojant – tikslingai atvirai kviečiant pateikti informaciją; asmenines patirtis; dokumentus; ar kitų įnašų“.

- 2018 m. „ABC Australia“ atliko didžiausią šalyje masinį tyrimą dėl senyvo amžiaus žmonių priežiūros, pasitelkdama „crowdsourcing“ teikti informaciją.
- Tyrimo ataskaitų teikimo padalinys CORRECTIV Vokietijoje sukūrė veiksmingą būdą įtraukti visuomenę į informacijos įvairiomis temomis per savo išbandytą „CrowdNewsroom“ platformą. Vienas sėkmingiausių iki šiol atliktų tyrimų buvo „Kam priklauso Hamburgas?”, kuris paragino Hamburgo piliečius atlikti atvirą tyrimą, kas iš tikrųjų valdo ir kontroliuoja nuomojamą nekilnojamąjį turtą neskaidrioje miesto nekilnojamojo turto rinkoje.
- „Bellingcat“ yra organizacija, kuri daugiausia dėmesio skiria internetiniams piliečių tyrimams ir dažnai naudojasi socialiniais tinklais, kad rinktų informaciją, dokumentuotų ir patikrintų įvykius kaip savo istorijų ir ataskaitų dalį. Pavyzdžiui, vienas iš pavyzdinių tyrimų, susijusių su Malaysia Airlines 17 (MH17) keleivinio lėktuvo numušimu Ukrainoje 2014 m., buvo labai priklausomas nuo „crowdsourcing“.

- Dokumentinio filmo apie šeimas, nukentėjusias nuo Meksikos narkotikų karo – „Anyone's Child Mexico“ – prodiuseriai rinko istorijas naudodamiesi nemokama telefono linija per vietines organizacijas ir paprašė žmonių visoje Meksikoje paskambinti ir papasakoti savo istorijas.

„Crowdsourcing“ *krizių nustatymui*

Ushahidi platformos naudojimas per 2010 m. Haičio žemės drebėjimą yra pirmasis atvejis, kai buvo naudojamas „crowdsourcing“ žemėlapis teikiant pagalbą nelaimių atveju. Nuo to laiko buvo sukurtos ir įdiegtos kelios kitos žemėlapių sudarymo platformos, skirtos humanitariniam atsakui, įskaitant kartu su kitomis technologijomis, pavyzdžiui, bepiločių orlaivių ar palydovinių vaizdų naudojimu.

- Čia pateikiamas 2019 m. pavyzdys, kai Indonezijoje rankų plovimo stotys buvo naudojamos, siekiant užkirsti kelią COVID-19 plitimui. Jame išsamiai aprašomos strategijos, naudojamos pritraukti naudotojus.

„Crowdsourcing“ *geresniam valdymui, atskaitomybei ir žmogaus teisėms*

„Crowdsourcing“ taip pat naudojo aktyvistai ir žmogaus teisių gynėjai korupcijos ir kyšių viešinime, kad padėtų gyventojams pranešti apie problemą savo valdžiai, ir paviešintų žmogaus teisių pažeidimus.

- 2017 m. Amnesty International ir Airwars bendro tyrimo dėl Rakos (Sirijoje) bombardavimo, kuriame dalyvavo daugiau nei 138 000 savanorių iš 124 šalių, pavyzdį.
- „ProPublica“ yra nepriklausoma, pelno nesiekianti redakcija, kurianti tiriamąją žurnalistiką. 2020 m. ji surengė bendradarbiavimu grįstą žiniasklaidos nušvietimą apie rinkimų dienos problemas visoje JAV, pavadintą ElectionLand, rinkdama duomenis iš rinkėjų žiniatinklio formų, tekstinių pranešimų, WhatsApp numerio ir bendradarbiaudama su elektronine apsaugos karštąja linija.

2 dalis: „Crowdsourcing“ reikalingų pastangų nustatymas

Prieš nusprendžiant įsitraukti į crowdsourcing, svarbu užduoti keletą klausimų. Klausimai diskusijoms pateikti žemiau:

- **Kodėl nori naudoti šį metodą?**
  - Pavyzdžiui, norite papasakoti istoriją / didinti informuotumą apie problemą, rinkti duomenis, kurie padėtų kitiems aktyvistams ar organizacijoms dirbti, įtraukti piliečius į svarbų procesą ar įvykį ar kt. Pavyzdžiui:
    - Masinė internetinė peticija, raginanti sukurti visame pasaulyje prieinamą koronaviruso vakciną
    - Tiesioginis oro kokybės žemėlapis visame pasaulyje

        - Platforma, skirta pranešti apie piliečiams rūpimus klausimus vietos valdžios institucijoms

- **Kokie yra pagrindiniai etikos sumetimai renkant įrodymus?**
    - Galbūt norėsite apsvarstyti tokius aspektus kaip informacijos tikslumas, bendraautorių privatumas, surinktų duomenų nuosavybė ir jūsų rezultatų prieinamumas.
    - Kai kurie iš šių aspektų taip pat gali turėti teisinių pasekmių, todėl prieš pradedant, gali būti protinga pasikonsultuoti su teisininku.

- **Kiek įmanoma patikrinti surinktus duomenis?**
    - „Crowdsourcing“ gali būti naudingas įrankis rinkti duomenis, kurių galbūt nežinote.
    - Tai taip pat gali būti sudėtinga patikrinti, ypač jei susiduriate su didesniais subjektais, kurie gali kurti robotus ir naudotojus, kurie gali sugadinti jūsų duomenis. Taigi, prieš pradėdami naudoti „crowdsourcing“, gerai pagalvokite, ar ir kaip būtų galima patikrinti duomenis, kuriuos rinktumėte.
    - Pateikite aiškų paaiškinimą, kokiu mastu galite patikrinti duomenis viešindami savo išvadas. Jei turite požymių, kad duomenys buvo tikslingai sugadinti, gerai pagalvokite, ar juos apskritai reikėtų viešinti. Pavyzdžiui:
        - Rusijos rinkimų pažeidimų kartografavimo platforma https://www.kartanarusheniy.org/ pateikia atsakomybės apribojimą, kuriame teigiama, kad pranešimus apie rinkimų pažeidimus naudotojai prisideda savanoriškai ir jie skelbiami be papildomo interneto svetainės administratorių patikrinimo, siekiant operatyviai atkreipti rinkimų administravimo įstaigų ir teisėsaugos dėmesį į duomenis (turinys rusų kalba).

- **Kas yra jūsų bendradarbiai?**
    - Apmokytų aktyvistų įnašų prašymas gali atrodyti kitaip nei bandymas sudominti paprastus piliečius.
    - Taip pat galite atsižvelgti į tokias demografines charakteristikas kaip bendraautorių amžius, lytis arba geografinė padėtis.
    - Jei nenorite, kad jūsų duomenys būtų gaunami tik iš vieno gyventojų pogrupio, paklauskite savęs, ar informacija apie jūsų pastangas gali pasiekti marginalizuotas grupes, ar jūsų naudojami įrankiai yra vienodai prieinami visiems, ar gali padidinti esamas skaitmenines spragas.
    - Galiausiai, nors duomenys gali būti nereprezentatyvūs sociologine prasme, vis tiek galite norėti, kad jie būtų iš įvairių vietų ir skirtingų grupių, kad su savo išvadomis pateiktumėte tikslesnį situacijos vaizdą.

- **Kas yra jūsų naudos gavėjai?**
    - Atminkite, kad tie papildomi duomenys ir galutiniai jūsų darbo naudos gavėjai gali skirtis.

- Stenkitės pateikti savo atradimus tokiu formatu, kuris būtų prieinamas auditorijai (-ėms), su kuria (-iomis) norite jais pasidalinti. Tai gali turėti įtakos formatui, kuriuo norite gauti duomenis. Pavyzdžiui:
  - Indijos korupciją sekančio projekto „I Paid a Bribe“ svetainė išryškina šalies žemėlapį pagal ataskaitų, gaunamų iš kiekvieno regiono, tankumą, skelbia atskiras ataskaitas realiu laiku, sumuoja jas pagal kategorijas ir pateikia apžvalgą.

- **Kokios kyla rizikos?**
  - Taip pat svarbu pagalvoti apie bet kokią riziką ar saugumo sumetimus, kurie gali turėti įtakos jums arba jūsų bendradarbiams ir ar jie apie tai žino.
  - Jei reikia, imkitės visų priemonių, kad apsaugotumėte jų privatumą ir anonimiškumą. Kartais tai gali reikšti, kad prieš tolesnį duomenų apdorojimą reikia imtis papildomų veiksmų, kad būtų “deanonimizuoti” duomenys.

- **Kas galėtų tapti jūsų partneriu ar bendradarbiu?**
  - Pagalvokite apie kitas grupes ar atskirus aktyvistus, kurie potencialiai domisi ar jau užsiima panašiu darbu. Ar yra kokių nors grupių, turinčių patirties rinkdami įrodymus arba kurių duomenis galite naudoti savo išvadoms susieti?
  - Paprastai yra gera idėja bendradarbiauti su kitais, kad padidintumėte savo pastangas arba išvengtumėte pasikartojimo.
  - Be to, bendradarbiaujant gali atsirasti įdomių mišrių duomenų rinkimo būdų. Pavyzdžiui:
    - „ProPublica“ projektas „Electionland“ sukurtas nušviesti kibernetiniam saugumui, dezinformacijai ir rinkimų vientisumui 2020 m. JAV rinkimuose. Siekdama dokumentuoti balsavimo kliūtis realiu laiku, organizacija subūrė daugiau nei 150 naujienų skyrių visoje šalyje koaliciją, taip pat paragino rinkėjus, apklausų darbuotojus ir rinkimų administratorius pranešti apie visas problemas, su kuriomis susiduria ar mato balsavimo proceso metu.

- **Kas atsitiks su duomenimis vėliau?**
  - Pavyzdžiui, ar norite atvirai dalytis neapdorotais duomenimis, ar parašyti ir platinti ataskaitą, pagrįstą savo išvadomis?
  - Ar labai svarbu nedelsiant pateikti išvadas?
  - Kokiu formatu turi būti pateikti duomenys? Pavyzdžiui:
    - „FixMyStreet“ JK skelbia apibendrintus duomenis apie problemas, apie kurias pranešė piliečiai, tiesioginėje informacijos suvestinėje, kurioje taip pat pateikiamos geriausios kategorijos, stebima, kiek ataskaitų jau buvo išspręsta, ir vertina vietos tarybas pagal jų reagavimą.

- **Ar reikėtų skirti vietos padėkoms ir kaip?**
  - Visada svarbu padėkoti, kai yra už ką ir kam.
  - Tai gali apimti padėką bendradarbiaujančioms organizacijoms, naudojamų įrankių ir programinės įrangos išvardinimą ir netgi bendradarbių (grupių ar

aktyviausių asmenų, ypač įdėjusių daug pastangų) įvardijimą, jei jiems nereikia / nenori likti anoniminiais.

- Visada pasitarkite su bendraautoriais, kaip jie nori būti įvardyti, arba pridėkite pastabą ir atsisakymą, kaip bus atliktas įskaitymas, įskaitant būdą žmonėms atsisakyti būti paminėtiems, jei tai jiems kelia pavojų. Pavyzdžiui:
  - Skelbdami savo išvadas apie civilių mirtį per 2017 m. bombardavimą Rakoje, Sirija, „Amnesty International“ ir „Airwars“ išvardijo visus partnerius, įrankius ir pagrindinius bendradarbius, pateikusius daugybę tyrime naudotų įrodymų (žr. https://raqqa.amnesty.org). / => „Įrankių rinkinys“ => „padėkos“).

3 dalis: tinkamo „Crowdsourcing“ metodo pasirinkimas

Tinkamo metodo pasirinkimas tikrai priklauso nuo jūsų tikslų.

Kartais žurnalistai sukuria saugų kanalą piliečiams anonimiškai siųsti patarimus, teisių gynėjai gali paskatinti aukas pateikti piktnaudžiavimo įrodymus bet kokiu jų turimu formatu, o rinkimų stebėtojai gali norėti, kad rinkėjai bandytų suskirstyti į kategorijas, kokio tipo pažeidimus jie liudija pagal kai kuriuos iš anksto nustatytus kriterijus.

Tai, kiek jums reikia crowdsourcing šaltinio duomenų, kad jie atitiktų griežtą analizei reikalingą formatą, nulems, ar turėtumėte rinkti struktūrizuotus, o ne nestruktūrizuotus duomenis.

- Kolumbijos universiteto Skaitmeninės žurnalistikos „Tow Center“ parengtame „Crowdsourcing“ vadove „atviri“ ir „konkretūs“ kvietimai prisidėti prie šių būdų:
  - „Atviro“ kvietimo metu visuomenė kviečiama įvairiais kanalais (el. paštu, telefonu, SMS, internetinės apklausos programine įranga ir kt.) susisiekti su žurnalistais su informaciją ir pateikti balsu, skambučiu pateikti naujienų organizacijai/žurnalistui. Šis formatas paprastai atitinka atvirojo duomenų rinkimo formatą.
  - „Specialiuose“ kvietimuose žurnalistai kreipiasi į tam tikras grupes, pateikdami konkretų informacijos prašymą. Informacija paprastai pateikiama iš anksto nustatytu formatu ir fiksuojama paieškos duomenų bazėje.

- Struktūrinio konkrečių duomenų sutelkimo privalumai apima konkrečių tipų įrodymų kaupimą vieningu formatu, kuris leidžia lengvai analizuoti duomenis. Tačiau griežtesnis formatas gali apriboti jūsų tikslinės auditorijos galimybę teikti duomenis.
- Atviri nestruktūrizuoti skambučiai leidžia gauti daugiau įvairių duomenų iš potencialiai didesnio skaičiaus bendraautorių, neapribojant savęs ir savo auditorijos pagal ataskaitų tipus, kuriuos, jūsų nuomone, galite gauti. Tuo pačiu metu tikrinti ir

analizuoti duomenis, gaunamus įvairiais kanalais įvairiais formatais, gali prireikti daug darbo ir laiko.

- Kartais gali būti naudojamas įvairių metodų derinys, ypač dideliuose bendradarbiavimo projektuose arba kai duomenis reikia susieti su įvairiais įrodymų srautais.

4 dalis. Darbas su tiksline(-ėmis) crowdsourcing šaltinių auditorija (-omis).

Sėkmingai įtraukti bendruomenės narius, kuriems norite teikti duomenis, yra pusė jūsų crowdsourcing sėkmės.

Kitaip tariant, jūs galite padaryti visa kita teisingai, bet jei niekas nepateiks jokių duomenų, visas jūsų darbas bus bergždžias. Todėl labai svarbu iš anksto pagalvoti apie bendruomenės įsitraukimą.

- Štai keletas naudingų orientacinių klausimų iš ProPublica:
  - Kas yra tie žmonės, kuriuos norite įtraukti? Kodėl jie yra geriausia bendruomenė?
  - Ką iš to gaus bendruomenė? Dėl kokių priežasčių kas nors dalyvautų?
  - Dėl kokių priežasčių kas nors nedalyvautų? Kaip planuojate numalšinti visus rūpesčius ir dvejones?
  - Kas labiausiai nukenčia? Kokia kalba jie apibūdina problemą? Ar jie pikti? Kur jie apie tai kalba? Kaip?
  - Kas yra įtakingiausi šios bendruomenės žmonės? Ar jau kalbėjote su jais? Ką jie mano apie idėją?

- Taip pat būtinai atsižvelkite į konkrečias socialines ir politines sąlygas, kuriomis dirbate.
  - Jei duomenų įnešimas yra susijęs su tam tikra rizika, žmonės nenorėtų to daryti, jei netikėtų, kad tai gali sukelti apčiuopiamų pokyčių.

- Pagalvokite apie tai, kaip galite **paskatinti narius domėtis** ir susižavėti dalyvavimu jūsų pastangose rinkti sutelktinius duomenis.
  - Kartais tai gali reikšti, kad prieš pasitelkiant crowdsourcing turėtų būti atliktas sąmoningumo ugdymo ir pasitikėjimo stiprinimo darbas.
  - Galite pasirinkti vykdyti informacinę kampaniją tam tikra problema, bendrauti su nuomonės lyderiais, stiprinti pasitikėjimą aktyviausiais bendruomenės nariais ir pan.

- Pagalvokite, kaip galėtumėte parodyti rezultatus, ir uždarykite grįžtamąjį ryšį su savo auditorija, net jei bendradarbiai lieka anonimiški. Pavyzdžiui:
  - galite nuspręsti paskelbti tiesioginius atnaujinimus apie savo sutelktinio šaltinio paieškos eigą arba netgi pasidalyti kai kuriais duomenimis, surinktais tais pačiais kanalais, kad paskatintumėte daugiau prisidėti (žr. toliau aprašytą atvejį „Kiekvieno vaikas: Meksika“, kur rasite puikų pavyzdį).
  - Taip pat naudinga užtikrinti, kad kai kurie įnašai būtų gauti kuo greičiau po to, kai pradėsite savo pastangas (tai gali būti iš anksto susitarta su kai kuriais patikimais šaltiniais, jei žinote, kad jie jau turi ką prisidėti).
  - **Trumpai tariant, kai bendruomenės nariai mato kitus aktyviai dalyvaujančius, jie labiau linkę įsitraukti patys.**

- Pagalvokite, kaip ketinate pasiekti savo auditorijas.
  - Geriau stengtis susisiekti per kanalus ir metodus, kurie labiau patinka jūsų tiksliniai bendradarbiai, o ne jūs.
  - Pavyzdžiui, tikslinė reklama internete naudojant tokius įrankius kaip „Facebook Lookalike Audiences“ gali būti labai galinga, tačiau tik tuo atveju, jei jūsų tikslinė auditorija pirmiausia naudoja „Facebook“ ir jei turite pakankamai išteklių išleisti „Facebook“ reklamai.
  - ProPublica siūlo keletą **naudingų pasiūlymų**, kuriuos reikėtų apsvarstyti renkantis susisiekimo metodą:
    - Kokia yra geriausia ir efektyviausia bendravimo su grupe forma? Kaip pranešite dalyviams, ką radote? Kiek norite/reikia, kad ši bendruomenė dalyvautų rengiant ataskaitas?
    - Ką norite, kad žmonės jums pasakytų? Ar bandote rinkti duomenis, anekdotų rinkinį, rinkti įrodomąją medžiagą ir pan.?
    - Kokią konkrečią informaciją jums reikia rinkti? Kaip dalyviui lengviausia tai jums duoti?
    - Jei šis projektas taps sulauks didžiulio atgarsio, kaip jį organizuosite? Ką reikia numatyti iš anksto?
    - Kaip ketinate panaudoti ar paskelbti tai, ką pateikia dalyviai? Kokius leidimus jie jau suteikia? Koks yra geriausias ir aiškiausias būdas pranešti apie savo ketinimus?

  - Štai keletas bendruomenės informavimo metodų ir kanalų, kuriuos galite apsvarstyti: (daugiau galite rasti atvejų tyrimuose, kuriuos cituoja Global Investigative Journalism Network):
    - Nyderlandų „De Correspondent“ reporteris Jelmeris Mommersas pasinaudojo naujienų svetaine, kad kreiptųsi tiesiai į „Shell“ darbuotojus dėl informacijos apie bendrovės žinias apie klimato kaitą. Jis pakvietė skaitytojus rašyti jam el. paštu ir gavo vidinius įmonės dokumentus ir kt.
    - JAV „ProPublica“ reporterė Adriana Gallardo bendradarbiavo su Nacionalinio visuomeninio radijo korespondente Renee Montagne, kad išplatintų internetinį klausimyną, skirtą moterims, patyrusioms gyvybei pavojingų gimdymo komplikacijų. „Facebook“ ir „Twitter“ bei netradicinėse vietose, pvz.,

sutelktinio finansavimo svetainėje „GoFundMe“, anketa davė tūkstančius atsakymų ir sukėlė daugybę istorijų.

- Dokumentinių filmų kūrėjai apie smurtą su narkotikais Meksikoje įkūrė nemokamą telefono liniją, kuri buvo skelbiama per vietinius partnerius, ir pakvietė žmones iš visos šalies skambinti ir papasakoti savo istorijas. Kai tai padarė, skambinantieji taip pat galėjo klausytis kitų pasakojimų. Dėl šių pastangų buvo sukurtas daugialypės terpės dokumentinis projektas „Anyone’s Child: Mexico“.

- Būtinai atsižvelkite į visus **privatumo ir saugumo** aspektus.
  - Ar jūsų tikslinei auditorijai gali kilti kokia nors rizika dalyvaujant jūsų crowdsourcing pastangose? Jei taip, labai svarbu padaryti viską, ką galite, kad pasiūlytumėte saugų ryšio kanalą ir apsaugotumėte savo bendradarbių tapatybę.
  - Nors žmonės gali būti nuolaidesni saugumui, nei jūs tikitės, turėtumėte stengtis užtikrinti, kad jie žinotų apie riziką ir apie tai, kiek galite ją sumažinti.

5 dalis: Techninių priemonių pasirinkimas crowdsourcing

Lengva pasijausti bejėgiu ir neišmanėliu dėl sunkiai perprantamo techninio įrankio, skirto duomenims gauti. Yra daugybė paprastų ir saugių įrankių, kuriuos sukūrė žmogaus teisių gynėjai, žurnalistai ar piliečių iniciatyvos. Tačiau svarbu pasirinkti tinkamą įrankį, kuris atitiktų jūsų crowdsourcing tikslus ir poreikius, o ne bandyti operaciją sukti aplink įrankį. Kartais tai gali reikšti, kad jums nereikia naujausių ir šauniausių technologijų, o pakaks naudoti paprastą telefono karštąją liniją, tekstinius pranešimus ar el. paštą

Norint pasirinkti geriausią variantą, svarbu atsižvelgti į:

- **Techninė aplinka**
  - Ar dauguma jūsų tikslinės auditorijos žmonių turi prieigą prie interneto? Koks jų ryšys?
  - Ar jie turi prieigą prie mobiliųjų įrenginių ar išmaniųjų telefonų, jei taip – kokio tipo / modelių žmonės dažniausiai naudojasi?
  - Taip pat atsižvelkite į jų kompiuterinio raštingumo lygį.

- **Privatumas ir sauga**
  - Svarbu pagalvoti, ar jūsų tikslinei auditorijai gali kilti kokių nors pavojų dalyvaujant crowdsourcing. Jei taip, labai svarbu padaryti viską, ką galima, kad pasiūlytumėte saugų ryšio kanalą ir apsaugotumėte savo bendradarbių tapatybę.
  - Nors žmonės gali būti nuolaidesni saugumui, nei jūs tikitės, turėtumėte stengtis, kad jie žinotų apie riziką ir apie tai, kiek galite ją sumažinti.

- **Esamų įrankių naudojimas ir kažko naujo kūrimas / pristatymas**
  - Žmonės ypač nenoriai keičia savo įpročius, susijusius su technologijomis. Ištirkite, kokius techninius įrankius jūsų tikslinė auditorija jau naudoja (t. y. socialinius tinklus, internetinius pasiuntinius ir pan.), ir apsvarstykite galimybę integruoti tuos įrankius.
  - Jei nuspręsite sukurti ir pristatyti specialų įrankį, skirtą duomenims gauti šioje konkrečioje aplinkoje, atsižvelkite į tai, kad nepaisant visų jūsų pastangų priversti žmones juo pasinaudoti gali prireikti šiek tiek laiko arba jums gali visai nepasisekti.

- **Kai kurios populiarios saugaus ryšio priemonės ir jų privalumai bei trūkumai**
  - Yra keletas saugių komunikacijos priemonių, kuriomis naudojasi žurnalistai ir aktyvistai. Nors nė viena sistema nėra 100% saugi, yra priemonių, kuriomis bandoma sukurti saugesnę aplinką, nei suteikia įprasti komunikacijos kanalai (pvz., telefonas, socialinė žiniasklaida, el. paštas).
  - Nė vienas įrankis nėra geriausias visiems, todėl svarbu atidžiai apsvarstyti individualias būsimo (-ų) bendradarbio (-ių) aplinkybes.

Įprasti komunikacijos kanalai apima:

Įrankiai	**Charakteristikos**	**Kompromisai**	**Atsisiuntimų ir sąrankos vadovai**
Signal https://signal.org/	Signal yra saugi ir patogi susirašinėjimo platforma, skirta iPhone ir Android, sukurta Open Whisper Systems. Jis užšifruoja visą ryšį nuo galo iki galo, todėl visi duomenys yra prieinami tik siuntėjui ir gavėjui.	Signal nėra toks populiarus kaip „WhatsApp“ ar kiti visiškai užšifruoti pranešimai, todėl vartotojai turi registruotis naudodami savo tikrus telefono numerius. Tačiau „Signal“ beveik neįrašo metaduomenų apie jūsų kontaktus ar pranešimus, todėl remiantis jūsų naudojimusi programa neįmanoma daryti išvados apie jūsų ryšį.	https://signal.org/download/
WhatsApp https://www.whatsapp.com/	Veikianti iPhone ir Android, populiari susirašinėjimo programėlė. Naudojama dviejų milijardų pasaulio gyentojų	Kaip ir „Signal“, „WhatsApp“ saugo vartotojų telefono numerius. Jis priklauso „Facebook“ ir dalijasi vartotojo telefono numeriu bei naudotojo analizės duomenimis su socialinės žiniasklaidos įmone. „Facebook“ taip pat gali būti priverstas dalytis savo naudotojų	https://www.whatsapp.com/download/

		duomenimis, reaguodamas į teismo įsakymą ar šaukimą į teismą. „WhatsApp“ taip pat gali kurti atsargines nešifruotų pranešimų kopijas „iCloud“ arba „Google“ diske – tai funkcija, kurią galima išjungti „Messenger“ saugos nustatymuose.	
Pretty Good Privacy (PGP) email šifravimas	PGP yra šifravimo standartas, populiarus tarp žurnalistų, siekiant apsaugoti el. Ji naudoja viešojo rakto kriptografiją, o tai reiškia, kad kiekvienas vartotojas turi „viešąjį raktą“, naudojamą kitiems vartotojams skirtiems pranešimams užšifruoti. Viešuoju raktu galima dalytis su bet kuo. Kiekvienas vartotojas taip pat turi atitinkamą „privatų raktą“, kuris naudojamas žinutėms iššifruoti ir jokiu būdu neturėtų būti bendrinamas. Tinka GPG Suite Mac, GPG4win for Windows and Linux, Thunderbird su Enigmail pratęsimu ir Mailvelope.	PGP reikalauja tam tikro lygio techninių žinių ir mokymo, kad įprastas kompiuterio ar išmaniojo telefono savininkas galėtų juo naudotis. Kiti saugūs ryšio kanalai gali pasiūlyti panašų apsaugos lygį ir būti patogesni vartotojui.	https://www.openpgp.org/software/
Protonmail https://proton.me/	ProtonMail yra nemokama PGP visiškai integruota nemokama el. pašto paslauga. Tai reiškia, kad naudojant ProtonMail, bet kas gali naudoti PGP, nepriklausomai nuo jų techninio išprusimo. Tai taip pat neleidžia niekam, įskaitant patį ProtonMail, skaityti ar dalytis jūsų el. laiškais ramybės būsenoje. Ši koncepcija vadinama nulinės prieigos šifravimu.	Nors ir nemokama (tik pagrindinė paskyra) ir paprasta naudoti, pagal numatytuosius nustatymus „ProtonMail“ bendrauja su išorinėmis el. pašto paskyromis be galutinio šifravimo. Taigi kitoje pusėje esantis išorinis el. pašto paslaugų teikėjas gali turėti prieigą prie el. laiškų, siunčiamų iš ProtonMail, todėl naudinga perduoti slaptą informaciją tik ProtonMail paslaugoje.	https://proton.me/pricing

SecureDrop https://securedrop.org	„SecureDrop“ yra atvirojo kodo pranešėjų pranešimų sistema, kurią gali įdiegti naujienų organizacijos, kad saugiai ir anonimiškai gautų dokumentus ir patarimus iš šaltinių. Jis pasiekiamas 20 kalbų ir naudojamas daugiau nei 50 naujienų organizacijų visame pasaulyje, įskaitant „The New York Times“, „The Washington Post“, „ProPublica“, „The Globe and Mail“ ir „The Intercept“.	Nors „SecureDrop“ leidžia bet kuriai jį įdiegusiai organizacijai visiškai valdyti serverius, sumažinti metaduomenis, užšifruoti duomenis ir taikyti daugybę kitų stiprių saugos metodų, jį nustatyti patiems gali būti brangu ir sunku.	https://docs.securedrop.org/en/stable/
Tella https://tella-app.org/	„Tella“ yra nemokama atvirojo kodo mobiliųjų duomenų rinkimo programa, skirta aplinkoms, kuriose yra ribotas interneto ryšys ir didelė saugumo rizika. Šiuo metu ji pasiekiama „Android“ įvairiomis kalbomis.	Nors „Tella“ yra gana paprasta naudoti ir ją galima pritaikyti prie ją naudojančios organizacijos poreikių, norint diegti programą, vis tiek reikia mokyti vartotojus ir tam tikrų techninių įgūdžių nustatant pagrindinį serverį.	https://tella-app.org/
FrontlineSMS https://www.frontlinesms.com	Įvairių organizacijų naudojama programinė įranga, skirta informacijai platinti ir rinkti siunčiant tekstinius pranešimus daugiau nei 120 šalių.	Naudoja paprastai prieinamą, bet ne saugų ryšio kanalą. Tai mokama paslauga su palyginti mažais mokesčiais.	https://www.frontlinesms.com/platform

6 dalis: patikrinimas ir patvirtinimas

Labai svarbu patikrinti iš crowdsourcing gautus duomenis. Atsižvelgdami į duomenų, kuriuos bandote rinkti, tipą ir formatą, gerai pagalvokite, kiek patikros norėtumėte ir galėsite atlikti.

Rezultatai gali atrodyti taip:

- **Nepatvirtinti duomenys**
  - Kai kurių duomenų gali būti neįmanoma patikrinti, nes jie gali būti nauji ir neturėti daug patvirtinančių šaltinių. Tokiu atveju galvokite ne apie patvirtinimą, o apie patikrinimą. Tai yra, pabandykite paneigti duomenis prieš paskelbdami.
  - **Jei negalite patvirtinti duomenų, bet vis tiek norite juos viešinti, pateikite aiškų atsakomybės atsisakymą, pažymėdami duomenis kaip „nepatvirtintus“.**

- **Iš dalies patvirtinti duomenys**
  - Nuspręskite, kiek patvirtinimo, jūsų nuomone, „pakanka“, kad duomenys būtų viešinami.

- **Pilnai patvirtinti duomenys**
  - Paprastai duomenys, kurie turi keletą patvirtinančių šaltinių.
    - Jei pranešama realiuoju laiku apie teisių pažeidimus arba kai apie incidentą reikia greitai paskelbti, kad būtų išvengta tolesnių nusikaltimų ar žalos, apsvarstykite galimybę vietoje suburti mobilią kvalifikuotų žmonių komandą, kuri galėtų apsilankyti įvykio vietoje ir surinkti patvirtinamuosius duomenis. įrodymus;
    - Kai neįmanoma patikrinti įkalčių vietoje, organizatoriai gali nuspręsti bendradarbiauti su vietoje veikiančiu asmeniu, su kuriuo jie gali pateikti nuorodas į savo išvadas.

Žemėlapių duomenų tikrinimas

Yra keletas elementų, į kuriuos galima atsižvelgti renkant informaciją per krizę. Ushahidi naudotojai per 2010 m. Haičio žemės drebėjimą nustatė šiuos duomenų tikrinimo būdus, įskaitant jų atvaizdavimą žemėlapyje:

- **lokacija** – ar pranešimas ateina iš tinkamos vietos?
- **Reputacija** – ar šaltinis, kuriuo pasitikiu aš arba žmonės, kuriais pasitikiu?
- **turinio palyginimas / agregavimas –** naudojant grupes ar kitus būdus, kaip atrasti modelius
- **laikas –** ar ataskaita ateina tinkamu laiku?

Informacijos tikrinimas socialiniuose tinkluose

Yra įvairių būdų, kaip patikrinti socialinės žiniasklaidos ataskaitas, daugialypės terpės failus ir kt., kuriuos galite naudoti, jei renkate tokio tipo duomenis (pvz., Europos žurnalistikos centro Socialinės žiniasklaidos patvirtinimo vadovas). Tačiau atminkite, kad patvirtinimo proceso nustatymas nėra lengva užduotis, todėl gali prireikti sukurti sudėtingą sprendimų medžio modelį ir tam tikrų įgūdžių turinčių žmonių komandą.

- Žiūrėkite šį žurnalistų pastangų stebėti ir tikrinti informaciją per 2012 m. Ukrainos parlamento rinkimus pavyzdį.

7 dalis: Duomenų analizė ir išvadų pristatymas

Svarbu sąžiningai ir teisingai pateikti iš crowdsourcing gautus duomenis, tačiau taip pat pagalvokite apie patrauklų jų pateikimo formatą.

- Prieš imdamiesi minios šaltinio, pagalvokite, kaip **analizuosite** ir **pateiksite** savo išvadas. **Formatas**, kuriuo norėtumėte pateikti savo išvadas, taip pat gali turėti įtakos formatui, kuriuo rinksite duomenis.
  - Pavyzdžiui, jei norite parašyti istoriją ar pasakojimų seriją, pagrįstą surinktais duomenimis, atviras nestruktūrizuotas skambutis gali būti tinkamiausias. Jei, priešingai, norėtumėte parašyti analitinę ataskaitą, jums gali prireikti sistemingesnių duomenų, kuriuos būtų galima analizuoti sistemingiau.
  - Net dirbdami su iš crowdsourcing gautais duomenimis vis tiek pagalvokite, kokį įspūdį norėtumėte padaryti su savo duomenimis; kitaip tariant, kokią „istoriją“ norėtumėte, kad jūsų duomenys papasakotų?

- Skelbdami išvadas, **apibūdinkite savo duomenų rinkimo metodus** ir tai, kaip padarėte išvadas (jei atliekate analizę).

- Nepamirškite **padėkoti** ten, kur tai daryti tinkama. Tai gali apimti padėką bendradarbiaujančioms organizacijoms, naudojamų įrankių ir programinės įrangos išvardinimą ir netgi bendradarbių (grupių ar aktyviausių asmenų, ypač didelių pastangų) įvardijimą, bet ne tų, kurie nori likti anonimiški.

- Svetainę ir bet kurią kitą medžiagą galite parengti remdamiesi savo išvadomis, aiškiai nurodydami, **ar galėjote patikrinti duomenis**, kuriuos gavote iš visuomenės, ir kokiu mastu.

Susiję šaltiniai: Exposing the Invisible straipsniai ir vadovai

- “It Takes a Crowd...”: Tips and examples of using crowdsourcing to collect information”, prie straipsnio taip pat pridedamas Exposing the Invisible Conference video pokalbis ir atvejo analizės vaizdo pristatymas)
- "Safety First!", vadovas iš Exposing the Invisible: the Kit.
- "Risk Assessment Is a Mindset, Not a Checklist", prie straipsnio taip pat pridedamas Exposing the Invisible Conference video.