MANUAL PËR SIGURINË DIXHITALE TË GAZETARËVE

Albanian Media Institute
Instituti Shqiptar i Medias

FRIEDRICH EBERT STIFTUNG

MANUAL PËR SIGURINË DIXHITALE TË GAZETARËVE

Albanian Media Institute
Instituti Shqiptar i Medias

FRIEDRICH EBERT STIFTUNG

Tiranë, 2023

Botues: Friedrich-Ebert-Stiftung
Office Tirana
Rr. Kajo Karafili
Nd-14, Hyrja 2, Kati 1,
Kutia Postare 1418
Tiranë, Shqipëri

Titulli i librit: Manual për sigurinë dixhitale të gazetarëve

Autor: Erlis Çela

Konsulent: Kejsi Bozo

Kopertina dhe layout: Bujar Karoshi

PËRMBAJTJA E LËNDËS

RRETH MANUALIT

Ky manual është konceptuar si një përpjekje për të rritur sigurinë dixhitale të gazetarëve shqiptarë. Synimi është rritja e ndërgjegjësimit e gazetarëve ndaj rreziqeve dhe kërcënimeve në hapësirën dixhitale dhe pajisja e tyre me njohuri dhe aftësi për të përballuar këto kërcënime. Manuali u drejtohet jo vetëm gazetarëve aktivë që janë të angazhuar pranë institucioneve të medias, por çdo personi të angazhuar në fushën e gazetarisë dhe medias, i cili jep ndihmesë në informimin e audiencave.

Manuali ofron njohuri për të rritur shkallën e dijeve të gazetarëve shqiptarë lidhur me konceptin e "sigurisë së gazetarëve" në përgjithësi dhe sigurisë dixhitale në veçanti. Për gazetarët është e rëndësishme të qartësohet se çfarë nënkuptohet me konceptin e sigurisë. Pavarësisht idesë së përhapur se kur flasin për sigurinë e gazetarëve, nënkuptojmë vetëm sigurinë e tyre fizike, në manual janë paraqitur qasje, përkufizime, modele konceptuale që e zgjerojnë dhe detajojnë konceptin e sigurisë së gazetarëve. Më pas manuali përqëndrohet në sigurinë dixhitale duke identifikuar rreziqet që burojnë nga ndërveprimi i gazetarëve me teknologjitë dhe platformat dixhitale, si dhe faktorët e riskut.

Në këtë pjesë janë identifikuar dhe shpjeguar kërcënimet dhe sulmet dixhitale më të përhapura me të cilat mund të përballen gazetarët. Po kështu bashkë me shpjegimet dhe përkufizimet për sulmet, ofrohen dhe këshilla praktike për t'u mbrojtur dhe për të adresuar problemin në përgjithësi. Ndërkohë, në pjesën e tretë, manuali përmbledh disa këshilla dhe hapa konkrete për t'u mbrojtur nga kërcënimet dhe sulmet dixhitale. Në pjesën e fundit ofrohet një listë me burime të vlefshme të cilat mund të konsultohen nga ana e gazetarëve për të thelluar njohuritë e tyre në fushën e sigurisë dixhitale dhe rritur aftësitë mbrojtëse në këtë drejtim.

HYRJE

Siguria e gazetarëve është e lidhur ngushtë me lirinë e shprehjes dhe lirinë e medias. Siguria për gazetarët mund të konceptualizohet në disa komponentë. Studime të ndryshme e kategorizojnë sigurinë e gazetarëve në dy dimensione. Së pari, në konceptin e sigurisë së gazetarëve kemi dimensionin personal, në të cilin përfshihet siguria fizike dhe siguria personale. Së dyti, në konceptin e sigurisë përfshihet dimensioni infrastrukturor. Në këtë dimension bën pjesë siguria dixhitale dhe siguria financiare. Koncepti i sigurisë, në vetvete, është mjaft kompleks dhe përbën një sfidë të vazhdueshme si për studiuesit, ashtu dhe për profesionistët e medias dhe politikëbërësit. Organizata të ndryshme, të angazhuara në monitorimin dhe kërcënimin ndaj sigurisë së gazetarëve, janë më tepër të fokusuara te siguria fizike. Në përgjithësi raportet që këto organizata publikojnë synojnë të dokumentojmë kërcënimet e drejtpërdrejta si vrasjet e gazetarëve, burgosjet, internimet e detyruara, kufizimet e ndryshme ligjore, etj.

Parë në aspektin e vlerësimit dhe matjes së nivelit të sigurisë të gazetarëve, kemi të bëjmë me dy qasje kryesore. Siguria mund të jetë objektive dhe subjektive. Kur diskutohet siguria sipas qasjes objektive atëherë

kemi të bëjmë me nivelin material, ndërsa kur flasim për qasjen subjektive, atëherë fokusi përqendrohet te niveli perceptues i sigurisë.

Kërcënimi i sigurisë së gazetarëve ka pasoja personale dhe sociale. Sa i përket pasojave personale, dihet që çdo kërcënim ndaj gazetarëve ndikon drejtpërdrejt në performancën e tyre dhe në produktivitetin profesional. Gazetarët e kërcënuar, të cilëve u cenohet siguria, pavarësisht së në çfarë dimensioni vjen kërcënimi, përbëjnë një tregues negativ për demokracinë dhe shoqërinë.

Në praktikë funksionimi i gazetarisë lidhet ngushtësisht me dy kategori të infrastrukturës. Së pari gazetaria varet nga infrastruktura financiare, e cila përbëhet nga burimet e të ardhurave, modeli ekonomik i mediave, etj. Së dyti varet nga praktika gazetareske që lidhet ngushtë me infrastrukturën dixhitale. Në ditët e sotme është gati e pakonceptueshme që rutina e një gazetari të jetë e pavarur nga infrastruktura teknologjike dhe dixhitale. Rrjedhimisht nëse kemi të bëjmë me sulme ndaj infrastrukturës dixhitale që përdorin gazetarët, kjo do të thotë se siguria është e kërcënuar. Nga ana tjetër është e kuptueshme që siguria dixhitale e medias, mund të kërcënohet nga rreziqe sa lokale aq edhe globale. Kjo do të thotë se kërcënimet në këtë drejtim mund të kenë natyrë mjaft komplekse dhe mund të përfshijnë aktorë që nuk lidhen thjesht me vendin apo shtetin ku ushtrojnë aktivitet gazetarët.

Në ditët e sotme sulmet kibernetike organizohen nga aktorë të ndryshëm, lokalë dhe ndërkombëtarë. Arsyet që i shtyjnë mund të variojnë nga ato më të thjeshtat që përfshijnë sulmet personale për qëllime hakmarrje, deri

te ato më të sofistikuarat, të cilat mund të kenë nga pas axhenda politike apo ideologjike. Shqipëria është tashmë një vend me përvojë në drejtim të rreziqeve kibernetike. Sulmet ndaj sistemit elektronik/dixhital të shtetit, të organizuara dhe mbështetura nga qeveria iraniane, përbëjnë shembullin më konkret në këtë drejtim. Këto sulme të hakerave iranianë nxorën në pah edhe një herë rrezikun për sigurinë dixhitale të qytetarëve dhe rëndësinë që ka marrja e masave të nevojëshme. Sigurisht që nga këto sulme, të kërcënuar janë edhe gazetarët shqiptarë. Ata mund të jenë të ekspozuar ndaj sulmeve në internet, që mund të synojnë të venë në pikëpyetje integritetin e tyre personal dhe profesional, si dhe mund të çojnë në kërcënim real fizik dhe psikologjik. Për këtë arsye është shumë e rëndësishme që gazetarët të kenë siguri dixhitale.

Nisur nga sa më sipër është parë i nevojshëm hartimi i këtij manuali, për t'i ardhur në ndihmë gazetarëve në Shqipëri, të cilët mund të përballen me rreziqe që kërcënojnë sigurinë e tyre dixhitale. Identifikimi i rreziqeve, faktorëve dhe aktorëve që kërcënojnë sigurinë dixhitale të gazetarëve përbën qëllimin e parë të këtij manuali.

Ndërgjegjësimi dhe edukimi i gazetarëve në drejtim të njohjes së faktorëve të riskut, ndihmon në rritjen e sigurisë së tyre. Qëllimi i dytë është rritja e njohurive dhe kapaciteteve të gazetarëve për t'u mbrojtur nga sulmet në hapësirën dixhitale. Ndërkohë që si qëllim final, mund të përcaktojmë ndihmesën në lirinë e medias dhe promovimin e gazetarisë së pavarur dhe të lirë.

KONCEPTI I SIGURISË SË GAZETARËVE

Koncepti i sigurisë për gazetarët mbetet një çështje komplekse. Varësisht nga konteksti më i gjerë shoqëror, koncepti i sigurisë për gazetarët mund të ndryshojë. Në vendet autoritare, apo gjysmë-autoritare, siguria për punonjësit e medias mund të lidhet më tepër me sigurinë fizike dhe mundësinë për të kryer aktivitetin profesional pa kufizime dhe penalitete. Ndërkohë që në zonat ku zhvillohen konflikte të hapura, luftëra dhe përplasje të armatosura, koncepti i sigurisë ngushtohet duke u përqendruar vetëm te siguria e jetës. Në interpretimin e saj më themelor, siguria nënkupton mungesën e dëmit të krijuar si pasojë e aktiviteteve që lidhen me raportimin e ngjarjeve nga gazetarët. Një grup studiuesish nga vende të ndryshme janë përpjekur të konceptualizojnë sigurinë e gazetarëve duke ofruar një kornizë të plotë të konceptit të sigurisë, rreziqeve dhe faktorëve të riskut. Sipas modelit të tyre konceptual, siguria e gazetarëve nënkupton masën në të cilën gazetarët mund të kryejnë detyrat e tyre të lidhura me punën pa u përballur me kërcënime për integritetin dhe mirëqenien e tyre *fizike, psikologjike, dixhitale dhe financiare*. Duke qenë se këto kërcënime përjetohen gjatë ose si rezultat i kryerjes së detyrave të tyre profesionale, të katër dimensionet – fizike dhe psikologjike, dixhitale dhe financiare – janë pjesë e sigurisë në punë të gazetarëve.

Në lidhje me sigurinë fizike të gazetarëve flitet shumë. Organizata të ndryshme bëjnë vlerësime periodike për sigurinë fizike të gazetarëve, duke raportuar për pozicionin e vendeve të raportuara për sigurinë e mediave dhe gazetarëve. Një nga indekset më të njohura është "Indeksi Botëror i Lirisë së Shtypit" i cili publikohet nga organizata "Reporterët pa Kufij". Ndërkohë në rajonin e Ballkanit perëndimor, platforma "Safejournalists.net" publikon një raport të përvitshëm për sigurinë e gazetarëve. Ky raport e ndan sigurinë e gazetarëve në katër tregues kryesore, ku secili nga treguesit ndahet në indikatorë të veçantë. Në treguesin "siguria aktuale" janë përfshirë komponentë si "kërcënime dhe ngacmime jo-fizike", "kërcënime ndaj jetës dhe sigurisë fizike të gazetarëve", "siguria aktuale" dhe "kërcënime dhe sulme ndaj medias dhe shoqatave të gazetarëve".

Përkufizimi që ky raport u bën kërcënimeve ndaj jetës dhe sigurisë fizike të gazetarëve nënkupton *"kërkesa për vrasjen e gazetarëve, miqve, familjes ose burimeve të gazetarëve, kërkesa për dëmtime fizike ndaj gazetarëve, miqve, familjes ose burimeve të gazetarëve. Këto kërcënime mund të bëhen drejtpërsëdrejti ose nëpërmjet palëve të treta, mund të dërgohen me komunikim elektronik ose ballë për ballë dhe mund të jenë të drejtpërdrejta ose të nënkuptuara"*[1]. Megjithëse Shqipëria nuk është një vend në konflikt dhe ka një kuadër ligjor optimal për ruajtjen sigurisë së gazetarëve, në raportet e organizatave të ndryshme brenda dhe jashtë vendit, janë evidentuar raste që kërcënojnë sigurinë fizike të gazetarëve. Të gjitha dimensionet që përbëjnë konceptin e sigurisë së gazetarëve janë të ndërlidhura me njëra-tjetrën. Një

[1] Tregues i Nivelit të Sigurisë së Gazetarëve në Ballkanin Perëndimor, Raporti përshkrues për Shqipërinë 2021, Blerjana Bino, Shoqata e Gazetarëve të Pavarur të Serbisë, 2021

gazetar që përballet me fushata linçuese në internet, të cilat përmbajnë gjuhë urrejtjeje, sulme fizike në vendin e punës, ambiente publike apo në banesë, apo dikush që përballet me kërcënime financiare, me siguri do të ketë pasoja psikologjike.

Siguria në punë			
Shtylla e parë: Siguria personale		**Shtylla e dytë: Siguria infrastrukturore**	
Dimensioni 1: **Fizike**	Dimensioni 2: **Psikologjike**	Dimensioni 3: **Dixhitale**	Dimensioni 4: **Financiare**
Ndikon në trupin e gazetarit	Ndikon në mirëqenien mendore dhe emocionale të gazetarëve	Ndikon në lirinë dixhitale dhe aftësinë për të përdorur mundësitë dixhitale	Ndikon në mbijetesën dhe aspektet profesionale të gazetarëve
Sulmet e dhunshme që kërcënojnë integritetin fizik, si vrasjet, torturat, dhe rrahjet	Agresioni verbal, gjuha e urrejtjes, përhapja e informacionit personal, ngacmimi (seksual, gjinor), përndjekja, kufizimet jo ligjore me qëllim „disiplinimin“ dhe censurimin e gazetarëve	Kërcënime për privatësinë dixhitale të gazetarëve, përfshirë sulmet “phishing”	Kërcënim për stabilitetin e punës.
Veprat që kërcënojnë lëvizshmërinë fizike, si rrëmbimet, arrestimet, ndalimet dhe burgosjet	Sulmet ndaj aftësisë për të kryer raportime, të tilla si frikësimi, detyrimi, ngacmimi në vendin e punës, bastisjet e zyrave dhe konfiskimet ose dëmtimi i pajisjeve	Survejimi dixhital, kufizimi i aksesit në informacion, hakerimi ose bllokimi i përmbajtjes dixhitale dhe kriminalizimi i sinjalizimit në hapësirën dixhitale	Kërcënim për zbatimin e praktikave/rutinave bazë gazetareske (burimi, verifikimi, prodhimi) dhe etikës. Konceptimi i rolit normativ (pushteti i katërt) kërcënohet të zëvendësohet nga ideologjia neoliberale e bazuarnëlogjikën e tregut Kërcënim në përzgjedhjen e temave dhe diversitetin e fuqisë punëtore[2]

[2] Vera Slavtcheva-Petkova, Jyotika Ramaprasad, Nina Springer, Sallie Hughes, Thomas Hanitzsch, Basyouni Hamada, Abit Hoxha & Nina Steindl, “Conceptualizing Journalists’ Safety around the Globe”, Digital Journalism, Jan 2023.

IDENTIFIKIMI DHE PËRKUFIZIMI I KËRCËNIMEVE

Studiuesit i përkufizojnë kërcënimet ndaj sigurisë së gazetarëve si veprime dhe kushte që rrisin rrezikun e dëmtimit fizik, psikologjik, dixhital dhe financiar ndaj gazetarëve si qenie njerëzore dhe si aktorë institucionalë. Siç mund të vihet re, ky përkufizim i kërcënimeve mbështetet në modelin konceptual të sigurisë së gazetarëve. Të gjitha kërcënimet, pavarësisht nga forma, natyra dhe burimet nga vijnë, rrezikojnë sigurinë në punë të gazetarëve dhe rrezikojnë potencialisht vazhdimin e kryerjes së detyrave gazetareske, si dhe autonominë, performancën e gazetarëve. Kjo nënkupton rrezikun ndaj aftësisë së gazetarëve për të përmbushur funksionet e tyre sociale. Kërcënimet janë gjithashtu një shkelje e rëndë e të drejtave individuale të njeriut, dhe të parimeve të transparencës dhe llogaridhënies. Ato minojnë të drejtën e njerëzve për t'u informuar, e cila për rrjedhojë zvogëlon nivelin e besimit në media dhe pjesëmarrjen në debatin publik aq thelbësor për funksionimin e demokracisë.

Kërcënimet fizike

Kërcënimet fizike mbeten më të thjeshtat për t'u perceptuar nga aktorët brenda dhe jashtë medias.

Identifikimi dhe raportimi i kërcënimeve fizike ndaj gazetarëve përbën një angazhim të rëndësishëm të organizatave dhe institucioneve që punojnë në fushën e mbrojtjes së gazetarëve dhe lirisë së medias. Kërcënimet fizike sipas qasjes së mësipërme "përfshijnë vrasje, rrahje, torturë, sulme seksuale dhe sulme të tjera të lidhura me punën, zhvendosje të detyruara, arrestime, ndalime, burgime, rrëmbime dhe zhdukje. Në listën e kërcënimeve fizike mund të përfshihen dhe kërcënime akute biologjike apo të lidhura me klimën, të tilla si rreziqet për shëndetin gjatë raportimit të ngjarjeve që lidhen me pandeminë COVID-19 apo mbulimin e fatkeqësive të ndryshme natyrore, si zjarret, termitet etj."

Kërcënimet psikologjike

Kërcënimet psikologjike janë më komplekse për t'u përkufizuar. Për shkak se kërcënimet psikologjike lidhen me gjendjen emocionale dhe mendore, identifikimi i tyre mbetet mjaft i vështirë. Në përgjithësi mendohet se kërcënimet psikologjike synojnë të prekin mirëqenien emocionale. Sipas studiuesve ato përfshijnë "frikësimin, shtrëngimin, zhvatjen, ngacmimin seksual, përhapjen e informacionit personal, gjuhën nënçmuese dhe gjuhën e urrejtjes, talljen dhe diskreditimin publik, kufizimet joligjore si pasojë e presionit publik, bullizmin në vendin e punës dhe detyrat që mund të shkaktojnë pasoja traumatizuese. Kërcënimet psikologjike lidhen gjithashtu edhe me sigurinë dixhitale. Një pjesë e këtyre kërcënimeve vijnë përmes burimeve dixhitale. Për shembull, frikësimi, kërcënimi për jetën, ngacmimet seksuale apo dhe bullizmi mund të vijnë përmes llogarive të ndryshme në median sociale, të cilat mund të jenë të identifikueshme ose anonime.

Kërcënimet dixhitale

Kërcënimet dixhitale përbëjnë një shqetësim në rritje jo vetëm për komunitetin e gazetarëve dhe punonjësve të medias. Secili nga ne që ndërveprojmë me internetin duke përdorur postën elektronike, apo duke komunikuar përmes mundësive që ofrojnë aplikacionet e ndryshme dhe platformat e medias sociale, mund të përballet me kërcënime dixhitale. Ato variojnë nga më të zakonshmet dhe më të thjeshtat për t'u adresuar, deri tek ato më komplekset që mund të përbëjnë krime penale dhe që kërkojnë angazhimin e profesionistëve të sigurisë dhe institucioneve të specializuara. Megjithatë në kontekstin e sigurisë së gazetarëve dhe medias, kërcënimet dixhitale mund të përfshijnë "sulme të ndryshme hakerimi dhe survejimi, kufizimin ose bllokimin e aksesit në informacion dhe burime, përndjekjet kibernetike (cyberstalking), sulmet "phishing", bullizmin kibernetik, trollingun, fushatat dezinformuese, etj.

Kërcënimet financiare

Grupi i katërt i kërcënimeve ka të bëjë me kërcënimet financiare. Kjo kategori e kërcënimeve lidhet drejtpërsëdrejti me mirëqenien e gazetarëve. Një gazetar që përballet me kërcënime financiare, nuk mund të jetë i lirë të ushtrojë profesionin e tij dhe të kryejë funksionet profesionale. Pasiguria financiare sfidon bazën operative të gazetarisë si institucion. Në nivel individual, pasiguria manifestohet në papunësi, humbje të të ardhurave ose pozicionit, pozitës profesionale dhe reputacionit. Gazetarët që e ushtrojnë profesionin në organizata mediatike, mbeten më të ekspozuar ndaj kërcënimeve financiare. Këto organizata dhe

kompani mediatike ndërtojnë modelin e tyre ekonomik dhe sigurojnë ekzistencën duke u bazuar në burime financiare te ndryshme. Në disa raste këto burime financiare përbëjnë dhe bazën e kërcënimeve për lirinë e medias dhe të gazetarëve. Ato mund të përbëjnë një nga faktorët e censurës apo vetëcensurës të gazetarëve. Nga ana tjetër, gazetarët e pavarur, të cilët nuk e ushtrojnë funksionin e tyre në varësi të organizatave dhe kompanive të medias, janë relativisht më të mbrojtur ndaj kërcënimeve financiare që burojnë si pasojë e marrëdhënieve financiare të medias me aktorë të fushave të tjera, si politika dhe biznesi. Megjithatë edhe për këtë kategori ekzistojnë rreziqe dhe pasiguri financiare të shumta, të cilat burojnë kryesisht nga mungesa e stabilitetit të burimeve financiare.

Aktorët dhe faktorët e riskut

Aktorët që përfshihen në kërcënime ndaj gazetarëve mund të klasifikohen në dy kategori kryesore. Kategoria e parë përfshin aktorët shtetërorë ose të lidhur me institucione shtetërore, ndërsa në grupin e dytë bëjnë pjesë aktorët joshtetërorë. Sigurisht që kjo përbën një ndarje në dy kategori mjaft të gjera. Nisur nga natyra dhe veçoritë e internetit dhe komunikimit dixhital, në disa raste identifikimi i aktorëve që përbëjnë kërcënim për gazetarët, bëhet shumë i vështirë. Një nga karakteristikat kryesore të komunikimit dixhital, që e vështirëson identifikimin e aktorëve përgjegjës për kërcënimet, është anonimiteti. Sa i përket faktorëve të riskut, studiuesit ofrojnë një kategorizim me tre grupe. Në grupin e parë bëjnë pjesë faktorët e rrezikut individual (niveli mikro), në grupin e dytë përfshihen

faktorët organizativë ose institucionalë (niveli i mesëm) dhe në të tretin faktorët shoqërorë (niveli makro). Ky model i kategorizimit të faktorëve mund të pësojë ndryshime varësisht kontekstit të gjerë shoqëror dhe politik të vendit. Për shembull në vendet me sistem politik jodemokratik, ku mungon shteti ligjor, faktorë si krimi, korrupsioni, dhuna dhe abuzimet e të drejtave të njeriut janë shpesh burime kërcënimi për median dhe gazetarët.

PERCEPTIMET E GAZETARËVE RRETH SIGURISË

Perceptimi i gazetarëve rreth sigurisë dixhitale dhe rëndësia që ata i kushtojnë kësaj çështje luan një rol të rëndësishëm në bashkëpunimin e aktorëve kryesorë që angazhohen në adresimin e kërcënimeve të kësaj natyre. Natyra e punës së gazetarëve dhe mënyra sesi ata kryejnë aktivitetin profesional, karakterizohet nga autonomia. Gazetarët brenda redaksive të medias nuk funksionojnë si vartës klasikë në një sistem organizativ të ngjashëm me bizneset apo organizatat e tjera. Pavarësisht se autonomia mbetet një nga vlerat më të rëndësishme dhe të domosdoshme për gazetarinë, ajo krijon sfida të shumta në kontekstin e sigurisë dixhitale. Sfida kryesore ka të bëjë me zbatimin e politikave të sigurisë, të cilat menaxherët i perceptojnë si një nga mjetet më të rëndësishme për formimin e kulturës së sigurisë organizative.

Aktorët e ndryshëm brenda organizatave të medias mund të kenë qasje dhe perceptime të ndryshme ndaj çështjeve të sigurisë. Këto dallime vihen re më së shumti mes stafeve teknike dhe gazetarëve apo redaktorëve. Në një kohë kur stafi teknik i organizatave mediatike i përcakton çështjet e sigurisë dixhitale si prioritare, gazetarët dhe redaktorët mund të mos ndajnë të njëjtin

qëndrim për këto çështje. Madje në disa raste mund të vihen re kundërshtime dhe rezistencë ndaj përpjekjeve nga lart-poshtë për të ndryshuar praktikat e sigurisë[3].

Studimet të ndryshme kanë zbuluar se mungesa e përgjithshme e kulturës së sigurisë në gazetari dhe konflikti midis gazetarëve dhe profesionistëve të IT-së brenda mediave janë ndër barrierat kryesore që pengojnë gazetarët të adoptojnë teknologjitë e sigurisë së informacionit. Nga ana tjetër gazetarët mund të kërkojnë këshilla për sigurinë e informacionit nga kontaktet jashtë medias ku janë të angazhuar, çka mund t'i ekspozojë organizatat e medias ndaj rreziqeve të ndryshme. Duke analizuar perceptimet e gazetarëve për kërcënimet e sigurisë dixhitale studiuesit i kategorizojnë kërcënimet duke u nisur nga: 1. Lloji i kërcënimit - Kërcënim ligjor, teknik apo fizik; 2. Nëse kërcënimi është përjetuar drejtpërdrejt nga gazetari apo nga një koleg i tij, ose është perceptuar si një rrezik i mundshëm-hipotetik; 3. Objektivi i kërcënimit - Kërcënim që ka si objektiv organizatën e medias, gazetarin individual apo burimin e gazetarit; 4. "Armiku" i përfshirë ose që dyshohet se është i përfshirë - kufizime ligjore, kompani, individë, etj.[4]

Megjithatë perceptimet mbi çështjet e sigurisë, ndryshojnë në varësi të profilit të punës së gazetarëve. Nga studime të ndryshme është vërtetuar se gazetarët investigativë janë më tepër të shqetësuar për

[3] Susan E. McGregor, Polina Charters, Tobin Holliday, Franziska Roesner, "Investigating the Computer Security Practices and Needs of Journalists", 24th USENIX Security Symposium,, 2015

4 Masashi Crete-Nishihata, Joshua Oliver, Christopher Parsons, Dawn Walker, Lokman Tsui & Ronald Deibert (2020), "The Information Security Cultures of Journalism", Digital Journalism, 8:8, 1068-1091.

survejimin-përndjekjen dhe kërcënimet ligjore nga aktorët shtetërorë, përfshirë agjencitë e zbatimit të ligjit dhe inteligjencës. Ndërkohë gazetarët që nuk janë të përfshirë në investigime shqetësohen më tepër për përgjimin, ngacmimet ose veprimet ligjore nga kompanitë ose individët të cilët mund të jenë subjekte të raportimit të tyre. Shpesh herë mungesa e kulturës së sigurisë në media dhe koordinimi apo mirëkuptimi i pamjaftueshëm ndërmjet stafeve të IT-së dhe gazetarëve, pengon adoptimin e teknologjive të sigurisë së informacionit në redaksi. Falë natyrës së fshehtë që kanë disa nga kërcënimet e sigurisë dixhitale, siç është survejimi dixhital i gazetarëve dhe sulmet e hakerimit ka gjasë që gazetarët të mos e kuptojnë se kur ata dhe/ose burimet e tyre janë në rrezik[5]. Për këtë arsye mbetet shumë e rëndësishme që të punohet në drejtim të rritjes së ndërgjegjësimit të gazetarëve për sigurinë dixhitale dhe në formimin e një kulturë të tillë në organizatat e medias.

[5] Jennifer R. Henrichsen (2019): "Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies, Digital Journalism.

PRAKTIKAT DHE SHQETËSIMET RRETH SIGURISË

Për të kuptuar më shumë mbi sigurinë dixhitale dhe kërcënimet me të cilat përballen gazetarët, është e nevojshme të identifikojmë praktikat gazetareske në të cilat, gjasat për rreziqe të sigurisë janë më të larta. Për këtë na vjen në ndihmë studimi me titull "Investigimi i praktikave dhe nevojave të gazetarëve të sigurisë kompjuterike", i autorëve Susan E. McGregor, Polina Charters, Tobin Holliday dhe Franziska Roesner[6]. Në këtë studim janë identifikuar disa praktika kryesore ku mund të shfaqen kërcënime të sigurisë dixhitale. Ndër më kryesoret mund të përmenden, gjetja e burimeve, komunikimi me burimet dhe ndërtimi i marrëdhënieve të besimit me burimet. Ndërkohë po i njëjti studim rendit si faktorë të rëndësishëm, mjetet e komunikimit që përdoren nga gazetarët, pajisjet dhe llogaritë, si dhe praktikat e menaxhimit të informacionit[7]. Në lidhje me gjetjen e burimeve të reja dhe komunikimin e gazetarëve me këto burime, në studim theksohen sfidat e ruajtjes së

[6] Susan E. McGregor, Polina Charters, Tobin Holliday, Franziska Roesner, "Investigating the Computer Security Practices and Needs of Journalists", 24th USENIX Security Symposium" 2015.

[7] Rubén Arnoldo González; Frida V. Rodelo "Double-edged knife:practices and perceptions of technology and digital security among Mexican journalists inviolent contexts, Tapuya: Latin American Science, 2020, Technology and Society.

informacioneve që shkëmbehen në një marrëdhënie të gjatë mes gazetarit dhe burimit. Nga ana tjetër dihet se gazetarët, për shumë arsye zgjedhin të komunikojnë me burimet e tyre përmes mjeteve që nuk kanë elementë të veçantë sigurie siç është: email, google docs, google drive, SMS, media sociale, aplikacione të ndryshme si Dropbox, Skype, Whatsapp, Viber, Signal, etj. Sidomos përdorimi i Google Drive që kërkon sinkronizim të të dhënave mund të paraqesë sfida të rëndësishme sigurie për mediat. Gazetarët kanë pak njohuri për përdorimin e mjeteve të sigurta, si mesazhet e enkriptuara.

Në përgjithësi, për zgjedhjen e teknologjisë së komunikimit gazetarët priren më së shumti nga vlerësimet se cila formë, pajisje, apo platformë është më e përshtatshme për burimin. Kjo nënkupton faktin se gazetarët lënë në plan të dytë kriterin e sigurisë kur bëhet fjalë për të komunikuar me burimet e informacionit. Në përgjithësi, praktikat e sigurisë kibernetike brenda organizatave të medias vuajnë si nga kufizimet e përdorshmërisë së mjeteve ekzistuese të sigurisë, ashtu edhe nga burimet e pamjaftueshme për të adresuar me përparësi çështje të sigurisë[8].

Shqetësimet kryesore të identifikuara nga gazetarët lidhen me tri kategori kryesore të kërcënimeve dixhitale. Këto tri kategori kërcënimesh janë kërcënimet që prekin burimet e gazetarëve, kërcënime që i drejtohen gazetarëve ose medias dhe kërcënime ndaj palëve të tjera.

[8] Susan E. McGregor*, Franziska Roesner, and Kelly Caine, "Individual versus Organizational Computer Security and Privacy Concerns in Journalism", 2016, Proceedings on Privacy Enhancing Technologies.

Kategoria e kërcënimeve	Shqetësimet
Kërcënime që prekin burimet e gazetarëve	Zbulimi nga ana e qeverisë ose institucioneve
	Masa disiplinore (humbja e vendit të punës)
	Reputacioni/pasojat personale
	Zbulim nga të tjerët që dëshirojnë të zbulojnë identitetin e burimit
	Rreziqe fizike
	Burgosje
Kërcënime që u drejtohen gazetarëve ose medias	Pasojat mbi imazhin dhe reputacionin (humbja e besimit nga ana burimeve)
	Informacion i rremë ose mashtrues nga një burim
	Kërcënimet fizike
	Pasoja financiare
	Dëmi i konkurrencës
Kërcënime ndaj palëve të tjera	Pasojat në marrëdhëniet politike
	Pasojat në marrëdhëniet e jashtme
	Të tjera

ÇFARË ËSHTË SIGURIA DIXHITALE?

Gazetarët përdorin një gamë të gjerë platformash online për të shpërndarë punën e tyre dhe për të komunikuar me burimet dhe audiencën. Platformat që lejojnë ndërveprimin me të tjerët, si mediat sociale, Wiki-t (wikipedia) që lejojnë redaktimin dhe plotësimin e përmbajtjes përmes bashkëpunimit dhe lejimit të aksesit për përdorues të ndryshëm, mund të përbëjnë sfida të sigurisë dixhitale për gazetarët. Termi siguri dixhitale apo siguri kibernetike përdoret për të përshkruar mekanizmat dhe praktikat mbrojtëse për identitetin në internet, të dhënat, rrjetet e informacionit dhe pajisjet në përdorim (email-et, kompjuterët, tabletat, telefonat, llogaritë e mediave sociale, të dhënat mjekësore dhe bankare, aplikacionet e komunikimit, etj.). Ndërkohë një term tjetër që përdoret në këtë fushë është "siguria në internet". Ky është një term më i gjerë që mund të përfshijë mungesën e ngacmimit dhe abuzimit në internet, ku përfshihen ngacmimet kibernetike, "trolling", etj. Në përgjithësi, siguria online ka të bëjë me shënjestrimin e një individi ose grupi në internet përmes sjelljeve të dëmshme.[9] Llojet e ngacmimeve në internet

[9] Arzu Geybullayeva; "Online Safety and Digital Security for all Journalists: A Prerequisite for Media Freedom", (OSCE) Representative on Freedom of the Media, 2022, Vienna, Austria.

mund të jenë të shumëfishta dhe të shumanshme. Ato përfshijnë, ndër të tjera, sulmet (DDoS), shpërndarjen e imazheve intime, talljen në internet, ngacmimin seksual në internet, dezinformimin, doxing[10], phishing, deepfake, hakerimin, etj.

Sfidat dhe rreziqet dixhitale me të cilat përballen gazetarët

Siguria dixhitale është një fushë mjaft e gjerë që përmbledh një sërë kërcënimesh, rreziqesh dhe mënyrash mbrojtjeje që zbatohen nga mediat dhe gazetarët në ditët e sotme. Në vija të përgjithshme, siguria dixhitale nënkupton mbrojtjen e linjave të komunikimit të gazetarëve, si dhe burimeve të tyre të informacionit nga sulmet dhe agresorët potencialë që veprojnë në hapësirën dixhitale ose që shfrytëzojnë teknologjinë dixhitale. Aktorë të ndryshëm, përfshi qeveritë apo institucione të ndryshme publike po përdorin gjithnjë e më shumë mjetet e përgjimit kibernetik. Këto mjete përfshijnë përgjimet e telefonave, hakerimin e email-eve dhe mesazheve SMS.

Gazetarët janë nën kërcënim të vazhdueshëm nga këto sulme, të cilat sa vjen dhe bëhen më të shpeshta. Çdo gazetar që ka në përdorim një telefon celular me të cilin kryen telefonata, që ka tablet për të shkëmbyer mesazhe përmes aplikacioneve, ose përpiqet të lidhë laptopin me një linjë interneti, është i ekspozuar ndaj këtyre kërcënimeve. Gazetarët mundet që përmes këtyre aktiviteteve rutinë të zbulojnë pozicionin e tyre dhe të lejojnë dikë të gjurmojë lëvizjet e tyre në hapësirën

[10] Shënim: Një praktikë e maskimit të sponsorit të një mesazhi për ta bërë atë të duket se rrjedh nga teksti

dixhitale[11]. Nëse komunikimi online i gazetarëve përfundon në duar të gabuara, ai mund të përdoret kundër tyre dhe mund të sjellë pasoja të rënda për vetë gazetarët apo burimet e tyre të informacionit.

Gjurmimi-Mbikëqyrja

Gjurmimi-Mbikëqyrja është një aktivitet që synon mbajtjen nën mbikëqyrje të gazetarëve dhe aktivitetit të tyre profesional. Ky proces përfshin përgjimin, mbledhjen dhe ruajtjen e informacionit që gazetari ka gjeneruar si rezultat i aktivitetit të tij profesional duke përdorur rrjetet e komunikimit. Ndërkohë që mbikëqyrja është ndjekja e një personi të caktuar, "mbikëqyrja masive" është mbikëqyrje në masë dhe pa dallim. Gjurmimi masiv përdor sisteme ose teknologji që mbledhin, analizojnë dhe/ose gjenerojnë të dhëna për një numër të pacaktuar ose të madh njerëzish, duke mos e kufizuar mbikëqyrjen tek individët për të cilët ka dyshime të arsyeshme për keqbërje. Vëzhgimi masiv njihet edhe si vëzhgim "pasiv" ose "i padrejtuar" drejt një individi të caktuar. Teknologjitë e gjurmimit dhe mbikëqyrjes janë të ndryshme dhe mund të përfshijnë gjurmimin e vendndodhjes, identifikimin e fytyrës dhe monitorimin masiv. Ekzistojnë gjithashtu metoda të përgjimit me shumicë për komunikimet me zë, SMS, MMS, email, faks dhe satelit[12].

[11] "Stayin Safe; A Protection Guide for Journalists in Kenya", Kenya Media Working Group, 2014.

[12] Jennifer R. Henrichsen, Michelle Betz, Joanne M. Lisosky, "Building Digital Safety for Journalism: A Survey of Selected Issues", 2015, Unesco.

Shfrytëzimet e softuerit dhe harduerit pa dijeninë e objektivit

Format e ndryshme të sulmeve dixhitale mund të jenë në funksion të njëra-tjetrës ose mund t'i hapin rrugë njëra-tjetrës. Për shembull, mjetet dhe teknologjitë e përdorura për të mbikëqyrur, gjurmuar dhe spiunuar gazetarët, mund të shërbejnë për të infektuar kompjuterët përmes viruseve apo të siç njihen ndryshe "Malware". Këto sulme, pasi arrijnë të infektojnë kompjuterët, lejojnë entitetet e jashtme të depërtojnë në rrjete kompjuterike specifike. Mjetet që lejojnë aksesin për monitorim dhe mbikëqyrje përfshijnë softuerët e ndërhyrjes, të cilët funksionojnë si vektorë sulmi. Vektorët e sulmit janë si kopje çelësash që ndihmojnë për të hyrë në një ndërtesë. E thënë ndryshe "exploit" është një mjet ose pjesë kodi që lejon një haker të shfrytëzojë një dobësi sigurie në harduerin (pjesët fizike) ose softerin (programet) e kompjuterit për qëllimet e veta. Kjo realizohet përmes shfrytëzimit të mangësive që kanë pajisjet ose programet kompjuterike. Në këtë mënyrë krijohet akses pa dijeninë e përdoruesit ose poseduesit të pajisjes. Një sulm i tillë shpesh përfshin gjëra të tilla si marrja e kontrollit të një sistemi kompjuterik, lejimi i përshkallëzimit të privilegjeve ose një sulm "DDoS". Me fjalë të tjera, disa exploits (shfrytëzime) janë të ngjashme me një hakerim. Nga ana tjetër, aktorë të ndryshëm mund të shënjestrojnë gazetarët për survejim duke instaluar një "çimkë" fizike ose një mikrofon të fshehur në pajisjet e komunikimit të një gazetari. Kjo mund të ndodhë në shtëpinë e gazetarit, ose në distancë, përmes dritareve duke përdorur mikrofonë me fuqi të lartë. Një gazetar mund të jetë subjekt i përgjimit, ku përmbajtja e telefonatave të tij dhe komunikimeve në internet mund

të monitorohet fshehurazi nga ata që dëshirojnë të kenë kontroll mbi to.

Sulmet e llojit "Phishing"

"Phishing" është një nga metodat më të zakonshme të sulmit. Ky lloj sulmi nënkupton një përpjekje për të aksesuar informacion të ndjeshëm dhe personal, zakonisht nëpërmjet email-eve, të cilat duket sikur vijnë nga një kompani e besueshme ose individ që ju e njihni, por në fakt është një uebsajt i rremë, i cili kontrollohet nga persona jo të besueshëm, të cilët kanë si synim vjedhjen e informacioneve[13].

Email-et "phishing" zakonisht kërkojnë të bëhet "përditësim" ose "të verifikohet" informacioni për llogarinë tuaj. Nëpërmjet këtij email-i të detyrojnë të klikosh në linkun që ata kanë vendosur në email për të bërë përditësimin sa më shpejt. Ky link të dërgon në faqen e tyre të ueb-it. Çdo informacion që ju shkruani ruhet nga këto persona në mënyrë që ta përdorin në momentin më të volitshëm me qëllime mashtrimi.

Llogaritë e kompromentuara

Llogaritë e përdoruesve, siç janë adresat e email-it, llogaritë e medias sociale, Skype, etj. mund të sulmohen përmes metodës "phishing", duke instaluar Malware në pajisjen e një gazetari dhe duke kompromentuar llogarinë e tij. Malware janë programe kompjuterike, të cilat instalohen në një kompjuter pa pëlqimin e

[13] Jennifer R. Henrichsen, Michelle Betz, Joanne M. Lisosky, "Building Digital Safety for Journalism: A Survey of Selected Issues", 2015, Unesco

përdoruesit dhe mund të kryejnë veprime të dëmshme siç janë vjedhja e fjalëkalimeve ose të dhënave të tjera që përdoren për të aksesuar një pajisje apo një llogari në internet. Ndërkohë që një gazetar është duke futur të dhënat e tij hyrëse, fjalëkalimin ose informacione të tjera të sensitive, ato mund të kapen nga këto programe duke kompromet uar llogarinë. Kompromet imi i llogarive mund të bëhet edhe duke përdorur një faqe interneti të rreme. Pasi përdoruesi të vendosë informacionin e tij hyrës, sulmuesi mund ta përdorë atë informacion për të hyrë në faqen e vërtetë të internetit, pa e paralajmëruar përdoruesin. Nëse përmes një sulmi arrihet të kompromet ohet llogaria e përdoruesit, p.sh duke vjedhur adresën e tij të email-it, atëherë personi/personat që e kanë marrë në kontroll këtë llogari apo adresë email-i mund të aksesojnë gjithë rrjetin kompjuterik dhe të kryejnë aktivitete të dëmshme. Autentifikimi me dy faktorë (Two-factor authentication) mund të ndihmojë në shmangien e kompromet imit të llogarive. Ndaj këshillohet që çdo gazetar dhe punonjës i medias që ka akses në rrjetin kompjuterik të redaksisë të aktivizojë "Two-factor authentication".

Sulmet me domain të rremë

"Fake domain attacks", i referohet situatave kur një sulmues krijon një uebsajt të rremë ose profil të rremë në mediat sociale që duket i ngjashëm ose identik me atë origjinalin, duke synuar:

- të mashtrojë përdoruesit që të ndajnë informacionin e tyre privat, si kredencialet bankare ose fjalëkalimet e tjera të llogarisë;

- të tërheqë lexuesit nga faqja origjinale e internetit dhe të shfaqë përmbajtje alternative të rreme;
- të krijojë pështjellim midis një komuniteti të synuar; ose
- të shërbejnë Malware për të kompromet uar audiencën e synuar të faqes origjinale.

Në të tilla raste sulmuesi përdorur një domain (emrin e faqes) të ngjashëm me origjinalin. Për shembull, nëse një sulmues do të krijojë një domain të rremë të ngjashëm me motorin e kërkimit Google, ai mund të ndryshojë ose shtojë një shkronjë (Gooogle) brenda fjalës duke bërë që përdoruesi të mos e kuptojë ndryshimin.

Sulmet "MitM"

Sulmet Man-in-the-Middle (MitM), të quajtura gjithashtu "sulme përgjimi", ndodhin kur sulmuesit futen në një transaksion komunikues mes dy palëve. Sulmet "MitM" përfshijnë një sulmues që përgjon komunikimin në rrjet për të përgjuar ose modifikuar të dhënat që transmetohen. Ndryshe nga trafiku i internetit, i cili zakonisht përdor HTTPS-në e koduar për të komunikuar, mesazhet SMS mund të përgjohen lehtësisht në aplikacionet mobile dhe për ta parandaluar mund të përdorin HTTP-në e kriptuar për të transmetuar informata potencialisht të ndjeshme. Sulmet "MitM" zakonisht ndodhin në celular kur lidheni në një rrjet jo të besueshëm ose të kompromet uar, siç janë rrjetet publike ose mobile Wi-Fi ose në situata kur aplikacione të njohura për ju përdoren për të ndërhyrë në sistemin tuaj.

Sulmet- "DoS" dhe DdoS"

"Sulm DdoS" ose "shpërndarje e mohimit të shërbimit" është sulmi kur hakerat në internet pushtojnë një rrjet ose serverët e tij duke dërguar shumë trafik. Me pak fjalë, krijojnë një situatë të ngjashme me trafikun në rrugë, gjë që shkakton bllokim të rrugëve. Në internet, ky sulm krijon trafik të madh dhe nuk lejon që rrjeti të trajtojë kërkesa të vlefshme duke nxjerrë jashtë përdorimi të gjithë sistemin (sulmet kur faqet nuk hapen, ose mezi hapen). Këto cilësohen njëkohësisht edhe si sulme nga shumë pajisje njëkohësisht.

Kompromet imi i përmbajtjes se faqes

"Defacement" në ueb është një sulm ku sulmuesit depërtojnë në një faqe interneti dhe zëvendësojnë përmbajtjen me mesazhet e tyre. Kjo metodë përdoret nga hakerat zakonisht për të demonstruar aftësitë e tyre të hakerimit ose për të arritur famë brenda komunitetit të tyre. Ata fitojnë kënaqësi duke anashkaluar masat e sigurisë dhe duke lënë gjurmët e tyre si dëshmi e aftësisë së tyre ose për t'i dhënë dikujt një mesazh.

Frikësimi, ngacmimi dhe ekspozimi i detyruar i rrjeteve online

Intimidimi dhe ngacmimet ndaj gazetarëve apo punonjësve të medias, nuk janë një dukuri e re që lidhet vetëm me natyrën dixhitale të komunikimit në ditët e sotme. Gazetarët në mbarë botën janë përballur dhe vazhdojnë të përballen me kërcënime, fyerje, ngacmime dhe presione nga më të ndryshmet që vijnë nga aktorë të identifikuar dhe të paidentifikuar. Megjithatë

kërcënimet dhe intimidimi në hapësirën dixhitale janë bërë një dukuri shqetësuese që kërcënon lirinë e medias dhe shënjestron gazetarët, të cilët punojnë për të zbardhur të vërtetat në emër të interesit publik. Kërcënimet në internet shpesh herë u paraprijnë sulmeve fizike. Ndaj është shumë e rëndësishme që gazetarët të cilët përballen me intimidim dhe kërcënime në median sociale apo në përgjithësi në internet, të mos i nënvlerësojnë këto situata dhe të kërkojnë menjëherë ndihmë. Në disa raste kërcënimet në internet kanë si synim detyrimin e gazetarëve që të zbulojnë të dhënat e llogarive të tyre në median sociale, apo të dhëna aksesi në email-e dhe databaza ku ruhet informacion i rëndësishëm[14].

Këto presione mund të vijnë edhe nga autoritet shtetërore dhe veçanërisht nga ato që merren me sigurinë. Qëllimi i këtij presioni mund të jetë detyrimi i gazetarëve që të zbulojnë fjalëkalimet e rrjeteve sociale apo pajisjeve që përdorin, në mënyrë që të kenë akses në komunikimet me burime dhe informacionet konfidenciale. Një mënyrë për të parandaluar këto situata është ndarja e informacionit me kolegë të besuar, të cilët mund të ndryshojnë të dhënat sapo të vihen në dijeni për arrestimin e kolegut të tyre apo presionin që ai mund të jetë duke përjetuar, me qëllim zbulimin e këtyre të dhënave. Në disa raste gazetarët zgjedhin të hapin llogari paralele për të ruajtur dhe shpërndarë informacionin. Kur një gazetar, për shkak të kërcënimit, detyrohet të tregojë të dhënat hyrëse të faqes së tij në Facebook apo çdo rrjet tjetër social, një llogari e dytë mund të shërbejë për të vazhduar aktivitetin.

[14] Jennifer R. Henrichsen, Michelle Betz, Joanne M. Lisosky, "Building Digital Safety for Journalism: A Survey of Selected Issues", 2015, Unesco

Fushatat dezinformuese

Fushatat dezinformuese ndaj gazetarëve janë një tjetër formë e sulmeve dhe kërcënimeve dixhitale. Ato synojnë të frikësojnë gazetarët, të shkatërrojnë kredibilitetin dhe integritetin e tyre profesional, si dhe të keqorientojnë audiencat. Për fat të keq shumë gazetarë në ditët e sotme përballen me fushata të tilla dezinformimi që përmbajnë shpifje, lajme të rreme dhe propagandë. Këto fushata sa vijnë dhe bëhen më të sofistikuara. Përdorimi i inteligjencës artificiale në deziformim po e bën më sfidues identifikimin dhe demaskimin e tyre. Gazetarët vihen në shënjestër duke u sulmuar me taktika dhe forma të ndryshme. Disa prej këtyre taktikave janë krijimi i faqeve apo llogarive të rreme në internet për të përhapur lajme të rreme ndaj gazetarëve, frikësimi dhe shantazhimi i gazetarëve duke përdorur foto ose video kompromentuese të manipuluara, klonimi i një faqeve interneti për të çorientuar audiencën, etj. Për t'u mbrojtur nga fushata të tilla dezinformimi nuk ekziston një zgjidhje përfundimtare dhe e plotë, megjithatë disa rrugë mund të jenë efikase për adresimin e problemit. Së pari është e nevojshme që gazetarët të tregojnë shkallë të lartë solidariteti ndaj kolegëve të tyre që përballen me të tilla fushata. Solidariteti i komunitetit të medias do të ndihmojë jo vetëm në demaskimin e fushatave dezinformuese, por gjithashtu edhe në dekurajimin e aktorëve që qëndrojnë pas tyre.

Së dyti është e nevojshme që gazetarët të rritin shkallën e njohurive dhe aftësive teknike për të identifikuar dezinformimin dhe demaskuar atë. Sa më shumë njohuri dhe aftësi praktike të kenë gazetarët për luftimin e lajmeve të rreme dhe fushatave të dezinformimit, aq më të mbrojtur do të jenë vetë ata dhe media në përgjithësi. Në

këtë pikë është e nevojshme që gazetarët dhe punonjësit e medias të trajnohen në mënyrë të vazhdueshme për t'u aftësuar në përdorimin e teknologjisë për të luftuar lajmet e rreme dhe format e tjera të dezinformimit.

Trolling-u, ngacmimet në internet

Ngacmimi online i gazetarëve është një formë e trolling. Trolling-u është konceptualisht jo shumë i qartë, megjithatë ky lloj sulmi mund të përkufizohet si një formë sjelljeje antisociale qëllimi i së cilës është të poshtërojë, provokojë dhe abuzojë me qeniet njerëzore. Ngacmimi në internet kundër gazetarëve përmban një sërë shprehjesh formash. Mesazhet nënçmojnë punën dhe identitetin social të gazetarëve me urrejtje dhe shpifje[15]. Trolling-u sjell pasoja negative në ndërveprimin mes audiencave dhe gazetarisë[16].

[15] Silvio Waisbord, "Mob Censorship: Online Harassment of US Journalists in Times of Digital Hate and Populism", 2020, Digital Journalism

[16] Silvio Waisbord, "Trolling Journalists and the Risks of Digital Publicity", 2020, Journalism Practice,

SI TË MBROHEMI?

Siguria kibernetike është thelbësore për gazetarët ashtu siç është për çdo profesion tjetër në epokën e sotme dixhitale. Gazetarët punojnë me informacione të ndjeshme, komunikojnë me burime në internet dhe përdorin platforma dixhitale për të publikuar punën e tyre. Për këtë arsye është e domosdoshme që gazetarët të informohen mbi disa procese dhe mjete kryesore që ndihmojnë për rritjen e sigurisë dixhitale. Disa nga këto mjete kanë të bëjnë me njohuritë për kriptimin e informacionit, aplikimin e faktorit të dyfishtë për aksesin e llogarive dixhitale dhe përdorimi i VPN-it (Virtual Private Network).

Kriptimi i informacionit

Kriptimi është një mjet mjaft i rëndësishëm për gazetarët. Nëse gazetarëve nuk u mundësohet komunikimi i sigurtë me kolegët dhe burimet e informacionit, ata do ta kenë të pamundur të kryejnë funksionin e tyre social në mënyrë të plotë. Ruajtja e anonimitetit të burimeve është gjithashtu mjaft e rëndësishme. Zbulimi i identitetit të burimeve si rrjedhojë e një komunikimi të pasigurtë në hapësirën dixhitale, do të ndikonte direkt në sigurinë e burimeve dhe në cilësinë e punës së gazetarëve.

Kriptimi si proces nënkupton ndryshimin e një mesazh origjinal (tekst i thjeshtë-plain text) me anë të një çelësi unik duke e kthyer atë në një "tekst i sigurt" (Ciphertext). Kjo bën që vetëm një person, i cili ka çelësin e kriptimit mund ta deshifrojë atë dhe ta kthejë në një formë të lexueshme. Duhet mbajtur parasysh se kriptimi funksionon në mborjtjen e përmbajtjes mesazhit, ndërkohë që nuk fsheh ato që njihen si "metadata" dhe që përfshijnë të dhënat mbi mesazhin. Në këto të dhëna bëjnë pjesë, numri i telefonit, ora dhe data e dërgimit, frekuenca e komunikimit, vendndodhja, etj. Kjo do të thotë se gazetarët duhet të jenë të vetëdijshëm për faktin se duke bërë kriptim të mesazhit nuk janë plotrësisht të sigurtë nga ekspozimi i të dhënave të tjera.

Ekzistojnë forma të ndryshme të kriptimit, të cilat kanë nivele të ndryshme mbrojtjeje. Një nga këto forma është kriptimi "end-to-end". Kriptimi "end-to-end" nënkupton faktin se vetëm dërguesi dhe marrësi kanë çelësin për të shndërruar një tekst të thjeshtë në një tekst të sigurtë dhe anasjelltas. Me pak fjalë dikush që mund të përgjojë mesazhet midis dy pajisjeve (si kompanitë e telekomunikimit) nuk mund të shohë përmbajtjen e tyre.

Përdorimi i VPN (Virtual Private Network)

Përdorimi i VPN-t kur je i lidhur në rrjet publik është shumë i rëndësishëm për gazetarët. Kjo bën të mundur kriptimin e trafikut. VPN funksionon si një tunel i kriptuar duke krijuar një lidhje të sigurtë. Duke komunikuar përmes VPN bëhet e mundur kriptimi në kohë reale i trafikut në internet dhe maskimi i identitetit të përdoruesit. Ofruesi i shërbimit të internetit ose

qeveria mund të kenë dijeni për lidhjen e një gazetari përmes VPN, por nuk mund të dinë se për çfarë po e përdor ai këtë rrjet. Ndërkohë duhet patur parasysh se ofruesi i shërbimit VPN mund të shohë të gjitha të dhënat e pakriptuara që po përdorin ose aksesojnë gazetarët.

Si funksionon një VPN dhe cilat janë përfitimet për gazetarët?

VPN shërben për të fshehur adresën IP duke e lënë rrjetin ta ridrejtojë IP-në përmes një serveri në distancë të konfiguruar posaçërisht dhe të drejtuar nga një host VPN. Kjo do të thotë që nëse shfletoni në internet me një VPN, serveri VPN bëhet burimi i të dhënave tuaja. Për rrjedhojë ofruesi i shërbimit të internetit (ISP-Kompania e internetit) dhe palët e tjera të treta nuk mund të shohin se cilat faqe interneti viziton një person ose çfarë të dhënash dërgon dhe merr ai. VPN funksionon si një filtër që i bën të gjitha të dhënat e përdoruesit më të vështira për tu aksesuar nga palët e treta që mund të jenë të intersuara për ti keqpërdorur ato.

Përfitmi kryesor i një lidhje VPN është maskimi i trafikut dhe të dhënave që shkëmbehen në internet duke i mbrojtur ato nga aksesi i jashtëm. Kjo përbën një ndihmë të madhe për gazetarët, pasi të dhënat e pakriptuara mund të shikohen nga kushdo që ka akses në rrjet. Ndërkohë një tjetër përfitim direkt që mund të arrihet me përdorimin e VPN-së është fshehja ose maskimi i vendndodhjes. Për shkak se të dhënat e vendndodhjes demografike vijnë nga një server në një vend tjetër, vendndodhja juaj aktuale nuk mund të përcaktohet.

Përdorimi i VPN i mundëson gjithashtu gazetarëve të kenë akses në përmbjatje lokale të faqeve të ndryshme. Disa faqe interneti ose shërbime të ndryshme përmbajnë

informacione që mund të aksesohet vetëm nga pjesë të caktuara të botës. Lidhjet standarde në internet përdorin serverë lokalë në vend për të përcaktuar vendndodhjen. Në këtë mënyrë aksesimi i përmbajtjeve të caktuara mund të mos jetë i mundur nga vendndodhja e përdouresit. Kështu, duke përdorur VPN, përdoruesi kalon një server të një vendi tjetër çka bën të mundur aksesimin e informacioneve ekzkluzive për përdoruesit e një vendi të caktuar.

Siguria në transferimin e të dhënave përbën një tjetër përfitim që mund të arrihet duke përdorur VPN. Shërbimet VPN lidhen me serverë privatë dhe përdorin metoda të kriptimit për të zvogëluar rrezikun e rrjedhjes së të dhënave.

Two-factor authentication

Me "Two-factor authentication" (2FA) nënkuptohet nevoja e një përdoruesi për një kredencial të dytë, krahas fjalëkalimit, për të aksesuar në llogaritë e ndryshme që disponon. Kjo metodë ndihmon në mbrojtjen e llogarive në përdorim nga kërcënimet dhe sulmet e ndryshme kibernetike. Për shembull, nëse llogaria e një gazetari sulmohet, sulmuesi nuk mund të identifikohet dhe të hyjë në llogarinë e gazetarit vetëm duke përdorur fjalëkalimin. Autentifikimi me faktorë të dyfishtë aplikohet si për adresat e postës elektronike, ashtu edhe për llogaritë që gazetarët kanë në platforma të ndryshme të medias sociale.

Përdorimi i 2FA së bashku me një menaxher për fjalëkalimet, rrit ndjeshëm nivelin e sigurisë dhe ofron mbrojtje nga sulmet që synojnë marrjen në kontroll të llogarive dhe keqpërdorimin e të dhënave. Niveli i

sigurisë mund të rritet edhe më tepër nëse të dy këto elementë (2FA dhe Menaxheri i fjalëkalimeve) përdoren në paisje të ndryshme. Për shembull, 2FA mund të përdoret përmes një aplikacioni që gjeneron kode në telefonin celular, ndërsa menaxheri i fjalëkalimeve mund të përdoret nga kompjuteri që disponon përdoruesi.

Menaxherët e fjalëkalimeve ndihmojnë në mbajtjen e llogarive tuaja më të sigurta duke gjeneruar fjalëkalime të gjata dhe unike për secilën prej llogarive. Ato gjithashtu bëjnë të mundur plotësimin automatik të fjalëkalimit në momentin që përdoruesi përpiqet të identifikohet. Kjo e bën edhe më praktik dhe lehtësisht të përdoreueshëm këtë mjet, pasi përdoruesi duhet të memorizojë vetëm një fjalëkalim që zhbllokon "kasafortën" e menaxherit të fjalëkalimit. Disa nga menaxherët e fjalëkalimeve më të njohura janë; "1Pasword", (ofron mundësi përdorimi pa pagesë për gazetarët), "Bitwarden" dhe "Dashlane". Është e rëndësishme që përpara se të zgjedhim një nga menaxherët e fjalëkalimeve të konsultohemi me burime të besuara për veçoritë dhe sigurinë që ofrojnë.

Ekzistojnë disa forma sesi mund të aplikohet 2FA. Një prej formave më të përdorura është aplikimi i faktorit të dyfishtë përmes numrit të telefonit. Sa herë që përdoruesi fut fjalëkalimin e saktë për të aksesuar llogarinë e tij, një kod i dytë "PIN" dërgohet me SMS në numrin e telefonit celular. Ky kod PIN përbën kredencialin e dytë që lejon përdoruesin të identifikohet përfundimisht dhe të ketë akses në llogarinë e tij.

Krahas aplikimit të faktorit të dyfishtë me ndihmën e numrit të telefonit, ekziston edhe mundësia përmes aplikacioneve mobile. Kjo formë funksionon në këtë mënyrë. Kur përdoruesi është duke hyrë në llogarinë e tij të gmail nga kompjuteri, ai do të marrë një njoftim

në aplikacionin e google në telefonin e tij celular, ku i kërkohet të konfirmojë nëse është ai personi që po tenton të aksesojë llogarinë.

Aplikimi i 2FA përmes aplikacioneve mobile që gjenerojnë kode, është një tjetër mënyrë. Në këtë rast përdoruesi duhet të shkarkojë në telefonin e tij një aplikacion që gjeneron kode. Disa prej aplikacioneve më të përdorura në këtë fushë janë; "Google Authenticator", "Authy", Microsoft Authenticator, LastPass Authenticator, etj.

KËSHILLA PRAKTIKE

Sigurimi i informacionit dhe pajisjeve

- Merrni parasysh mbajtjen e informacionit tuaj konfidencial në një disk të jashtëm dhe në disa kopje rezervë. Kjo do t'ju sigurojë që të ruani dhe aksesoni informacionin edhe pas një sulmi hakerimi nga i cili mund të keni humbur aksesin në pajisjen tuaj apo llogarinë e postës elektronike.

  Kriptoni (kodoni) informacionin e ruajtur në pajisje të jashtme. Kjo masë mund të ndihmojë në ruajtjen e informacionit edhe nëse pajisja juaj është vënë nën kontroll nga sulmues të ndryshëm, të cilët kanë arritur aksesin në të përmes rrugëve të ndryshme të jashtëligjshme. Kriptimi i informacionit është i rëndësishëm edhe në rastet kur ju po e ndani atë me llogari të tjera të besuara në mënyrë që të ruani kopje që mund të përdoren pas sulmeve të ndryshme dixhitale. Trafiku i koduar i ngjason letrës në një zarf shumë të sigurt; kushdo mund të shohë se nga vjen dhe ku po shkon, por vetëm pajisja juaj dhe faqja e internetit me të cilën po komunikoni mund të hapin zarfin, për të parë se çfarë ka brenda[17].

[17] Susan Mcgregor, "Digital Security and Source Protection for Journalists", 2014, Tow Center for Digital Journalism.

- Gazetarët duhet të kenë parasysh se përveç komunikimeve, ata mund të kriptojnë gjithë hard-diskun duke përdorur "Bitlocker" në Windows dhe "Firevault" për Mac.
- Sigurohuni që kompjuteri juaj të jetë i fikur kur largoheni nga zyra, apo vendi ku punoni. Fikja e pajisjes është një masë shtesë që mbron pajisjen dhe informacionin që ndodhet në të, si dhe komunikimet e gazetarëve, duke ndërprerë lidhjen me rrjetin e internetit.
- Këshillohet që gazetarët të mos përdorin kompjuterët në vende publike siç janë ambientet ku ofrohet shërbim interneti (Internet caffe), hotele apo vende të ngjashme, për biseda konfideciale apo për të komunikuar më burimet e tyre. Nëse jeni të detyruar t'i përdorni këto pajisje, atëherë sigurohuni që fillimisht të keni shkarkuar "Ccleaner" ose një program të ngjashëm në një USB për ta aplikuar në këto pajisje përpara përdorimit. Ccleaner është një program që do të mund të pastrojë kompjuterin nga skedarët e browser-it që gjurmojnë aktivitetin tuaj në internet.
- Përpiquni të shmangni lidhjen me rrjete WiFi në ambiente si aeroporte, sheshe publike, kafene apo ambiente të ngjashme ku lidhja ofrohet pa pagesë dhe ku mund të lidhen njëkohësisht një numër i madh përdoruesish. Nëse jeni të detyruar për shkak të emergjencës së punës për të përdorur këto rrjete, atëherë sigurohuni të përdorni shërbimin VPN. Nëse kemi të bëjmë me një sulm "Man in the Midle", përdorimi i VPN e bën të pamundur që një haker i cili mund të jetë i lidhur në të njëjtin rrjet, të ndërhyjë në komunikimin tënd.

Fjalëkalime të sigurta

- Konfiguroni gjithmonë laptopin apo kompjuterin tuaj me një fjalëkalim sa më të sigurt. Sigurohuni që këto fjalëkalime të jenë sa më të sigurta dhe të përmbajnë simbole, numra dhe një përzierje e shkronjave të mëdha dhe të vogla.
- Tregohuni vigjilentë në ambientin e punës për mos lejuar persona të ndryshëm të shikojnë, lexojnë mesazhet, apo fjalëkalimet e llogarive tuaja. Edhe pse duket si një këshillë bazike, neglizhenca në këtë pikë është e madhe nga ana e gazetarëve. Në disa raste gazetarët tregojnë besim të tepruar ndaj njerëzve të njohur brënda redaksisë. Ky besim i tepruar mund t'i hapë rrugën personave që mund të kenë qëllime negative, duke rrezikuar jo vetëm aksesimin e të dhënave por edhe ekspozimin e burimeve të gazetarit ndaj rreziqeve të shumta.

Siguria e emailit dhe komunikimit

- Përdorni gjithmonë adresa email-i të mbrojtura. Për t'u siguruar se shërbimi që përdorni mbron komunikimet tuaja nga ndërmjetësuesit e tjerë, kontrolloni adresën e uebit në krye browser-it tuaj. Sigurohuni që adresa të fillojë më "https://" dhe jo me "http". Dallimi midis këtyre dy protokolleve qëndron në faktin se "https" përdor TLS (SSL) për të kriptuar informacionin duke ndihmuar në shmangien e mbikëqyrjes dhe gjurmimit. Nëse lidheni me një faqe interneti nëpërmjet http, është më shumë se dërgimi i informacionit tuaj nëpërmjet qindra kartolinave. Në këtë rast, çdo hallkë që e trajton këtë informacion mund të shohë se nga vjen dhe ku po shkon. Përmbajtja e mesazheve tuaja mund të lexohet nga kushdo[18]. Mund të përdorni

[18] Susan Mcgregor, "Digital Security and Source Protection for Journalists", 2014, Tow Center for DigitalJournalism

programin pa pagesë “Veracrypt” për kriptimin e disqeve të jashtme.

- Shërbime të tilla si Twitter, Facebook dhe Hotmail i Microsoft-it tani e ofrojnë këtë si një veçori sigurie falas, por opsionale.
- Siguroni mesazhet tuaja. Ka shumë platforma dhe aplikacione që ofrojnë më shumë siguri për mesazhet. Është e rëndësishme që gazetarët të komunikojnë me burimet e tyre përmes aplikacioneve që ofrojnë komunikim të kriptuar (koduar). Ndonëse asnjëherë nuk ka siguri maksimale për mesazhet e shkëmbyera në aplikacionet mobile, disa prej tyre ofrojnë më shumë garanci në këtë drejtim. Aplikacione të tilla si Skype, Signal, Whatsapp janë disa prej aplikacioneve që ofrojnë kriptimin e komunikimeve. Për rastin e Whatsapp-it ka diskutime lidhur me sigurinë që ofron për kodimin e mesazheve. Këto diskutime burojnë nga fakti se aplikacioni është pjesë e “Meta”, grupi i madh që përfshin edhe platformat Facebook dhe Instagram. Gjithashtu është e rëndësishme që gazetarët të aktivizojnë “zhdukjen e mesazheve”.

Siguria në internet dhe median sociale

- Një nga elementët më të cenueshëm në kuadër të sigurisë dixhitale janë llogaritë në median sociale. Gazetarët duhet të rishikojnë rregullisht opsionet e privatësisë dhe sigurisë në median sociale. Është e rëndësishme që të jeni të qartë se cilat të dhëna pranoni që të jenë të disponueshme për publikun.
- Kufizoni informacionin personal që shpërndani në platformat e mediave sociale. Jini të kujdesshëm në pranimin e kërkesave për miq/ndjekës nga individë të panjohur. Rregulloni cilësimet tuaja të privatësisë për të kontrolluar se

kush mund t'i shohë postimet dhe informacionet tuaja.

- Gazetarët duhet të kërkojnë në mënyrë periodike për emrin dhe të dhënat e tyre në internet. Përdorni të gjithë motorët e komunikimit që njihni për të parë se çfarë informacioni rreth jush qarkullon në internet dhe kush e ka publikuar atë. Një rrugë e duhur për ta bërë këtë është të konfigurosh "Google Alerts" me emrin tënd. Në këtë mënyrë do të njoftohesh automatikisht sa herë emri dhe të dhëna të tjera rreth jush publikohen në internet.
- Mbroni llogaritë tuaja duke aktivizuar aksesin më llogari përmes "Two-factor authentication". Forma më tradicionale për ta bërë këtë është përmes mesazheve në celularin tuaj. Ndërkohë gazetarëve u sugjerohet të përdorin aplikacione të tilla si "Authy". Madje për raste kur gazetari ndihet i kërcënuar seriozisht për hakerim, sugjerohet të përdorin dhe një çelës fizik sigurie si "YubiKey". YubiKey, është një pajisje e vogël që ngjason me një USB. Ju mund të eksploroni edhe alternativa të tjera për çelësat e sigurisë.
- Informoni burimet tuaja për kanalet e sigurta të komunikimit. Megjithëse shpesh gazetarët ngurrojnë t'u japin detaje burimeve të tyre rreth komunikimit të sigurt dhe rreziqeve të ndryshme, është e rëndësishme që nëse po komunikoni për një çështje të ndjeshme ta informoni burimin për masat që keni marrë me qëllim garantimin e një komunikimi të sigurt.

Trajnoni ekipin tuaj

- Nëse punoni me një ekip, sigurohuni që ata të jenë të udhëzuar edhe për praktikat më të mira të sigurisë kibernetike. Trajnimet duhet të jenë të planifikuara dhe periodike. Këto trajnime

mund të përfshijnë edhe simulimin e sulmeve të ndryshme kibernetike.

Plani i reagimit ndaj sulmit

- Zhvilloni një plan për t'iu përgjigjur një incidenti ose sulmi kibernetik. Është e rëndësishme ta keni të qartë se çfarë duhet të bëni nëse dyshoni për një shkelje ose akses të paautorizuar.
- Hapi i parë është ruajtja e qetësisë dhe shmangia e panikut në raste sulmi.
- Dilni nga llogaritë e Google, Facebook (të gjitha rrjetet sociale që keni në përdorim, WhatsApp, etj., në të gjitha pajisjet.
- Kontrolloni për emaile të llojit "password reset" në rast se sulmuesi ka tentuar të nderrojë passwordet tuaja.
- Nëse përdorni të njëjtat kredenciale për shumë llogari, ndryshoni edhe fjalëkalimet për secilën prej këtyre llogarive.
- Kërkoni ndihmën e ekspertëve të besuar!

Mbrojtja ligjore

- Njihuni me mbrojtjen dhe të drejtat ligjore në dispozicion të gazetarëve sipas legjislacionit vendas dhe ndërkombëtar. Kjo mund të jetë thelbësore në rast mosmarrëveshjesh ligjore ose kërcënimesh që lidhen me punën tuaj. Mos harroni se siguria kibernetike është një proces i vazhdueshëm dhe kërkon vigjilencë dhe përshtatje ndaj kërcënimeve të reja. Duke zbatuar këto praktika më të mira, ju mund të mbroni më mirë veten, burimet tuaja dhe punën tuaj si profesionist i medias.

BURIME TË VLEFSHME

- Resources for protecting against online abuse https://cpj.org/resources-for-protecting-against-online-abuse/
- Digital Safety Kit https://cpj.org/2019/07/digital-safety-kit-journalists/#protect
- The Rory Peck Foundation - Digital Security Guide https://rorypecktrust.org/how-we-help/freelance-resources/digital-security/
- GCA Cybersecurity Toolkit https://gcatoolkit.org/mission-based-orgs/
- The Journalist Security Assessment Tool https://advisory.gijn.org/cybersecurity-assessment/
- How Journalists Can Prepare for Online Harassment, Disinformation- https://gijn.org/2021/02/24/preparing-for-disinformation-campaigns-and-online-harassment/

- A Guide to Doxxing Yourself on the Internet https://docs.google.com/document/d/1WleGh4D3_p7TYPhjfKRHQyMYwhZayYZayYY7AZSSzPs/edit#heading=h.lamti05zshb8
- Social Media Security & Privacy Checklists https://docs.google.com/document/d/1ud1ILFkIG0BeLX9jlzJMxCPm8-cSeqPjU60nkhUPYA8/edit#heading=h.w98iq6r1yct2
- Safety Notes- https://cpj.org/safety-notes/

REFERENCA

1. Tregues i Nivelit të Sigurisë së Gazetarëve në Ballkanin Perëndimor, Raporti përshkrues për Shqipërinë 2021, Blerjana Bino, Shoqata e Gazetarëve të Pavarur të Serbisë, 2021
2. Vera Slavtcheva-Petkova, Jyotika Ramaprasad, Nina Springer, Sallie Hughes, Thomas Hanitzsch, Basyouni Hamada, Abit Hoxha & Nina Steindl, "Conceptualizing Journalists' Safety around the Globe", Digital Journalism, Jan 2023
3. Susan E. McGregor, Polina Charters, Tobin Holliday, Franziska Roesner, "Investigating the Computer Security Practices and Needs of Journalists", 24th USENIX Security Symposium, 2015
4. Masashi Crete-Nishihata, Joshua Oliver, Christopher Parsons, Dawn Walker, Lokman Tsui & Ronald Deibert (2020), "The Information Security Cultures of Journalism", Digital Journalism, 8:8, 1068-1091
5. Jennifer R. Henrichsen (2019): "Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies, Digital Journalism.
6. Rubén Arnoldo González; Frida V. Rodelo "Double-edged knife: practices and perceptions of technology and digital security among Mexican journalists in violent contexts, Tapuya: Latin American Science, 2020, Technology and Society

7. Susan E. McGregor, Franziska Roesner, and Kelly Caine, “Individual versus Organizational Computer Security and Privacy Concerns in Journalism”, 2016, Proceedings on Privacy Enhancing Technologies

8. Arzu Geybullayeva; “Online Safety and Digital Security for all Journalists: A Prerequisite for Media Freedom”, (OSCE) Representative on Freedom of the Media, 2022, Vienna, Austria,

9. Stayin Safe; A Protection Guide for Journalists in Kenya”, Kenya Media Working Group, 2014

10. Jennifer R. Henrichsen, Michelle Betz, Joanne M. Lisosky, “Building Digital Safety for Journalism: A Survey of Selected Issues”, 2015, Unesco

11. Silvio Waisbord, “Mob Censorship: Online Harassment of US Journalists in Times of Digital Hate and Populism”, 2020, Digital Journalism

12. Silvio Waisbord, “Trolling Journalists and the Risks of Digital Publicity”, 2020, Journalism Practice

13. Susan Mcgregor, “Digital Security and Source Protection for Journalists”, 2014, Tow Center for Digital Journalism

14. Susan Mcgregor, “Digital Security and Source Protection for Journalists”, 2014, Tow Center for Digital Journalism