Konsiderata mbi Votimin përmes Internetit:

Një pasqyrë për marrësit e vendimeve zgjedhore

Dokumenti i bardhë i IFES

Prill 2020

USAID
FROM THE AMERICAN PEOPLE

Canada

UKaid
from the British people

International Foundation for Electoral Systems
IFES
30 Years

Konsiderata mbi Votimin përmes Internetit: *Një pasqyrë për marrësit e vendimeve zgjedhore*

Pril 2020

Meredith Applegate
Këshilltare Programi e IFES, Ukrainë

Thomas Chanussot
Ekspert i lartë i Teknologjisë dhe Sigurisë Kibernetike të zgjedhjeve

Vladlen Basysty
Menaxheri i IFES për Teknologji dhe Siguri Kibernetike, Ukrainë

Autorët falemnderojnë Peter Erben, Ronan McDermott,
Dr. Beata Martin-Rozumiłowicz, Dr. Staffan Darnolf dhe Olha Antonova për kontributet dhe shqyrtimet e tyre
.

Konsiderata mbi Votimin përmes Internetiti: Një Pasqyrë mbi Marrësit e Vendimeve Zgjedhore

Fondacionin Ndërkombëtarë për Sistemet Zgjedhore
2011 Crystal Drive, Kati i 10-të
Arlington, VA 22202 Email:
editor@ifes.org Fax:
202.350.6701

Ky raport është bërë i mundur nga mbështetja e Çështjeve Globale të Kanadës, ndihma e MB dhe Populli amerikan përmes mbështetjes të Agjencia e Shteteve të Bashkuara për Zhvillim Ndërkombëtar (USAID). Mendimet e shprehura këtu janë të autorit dhe jo domosdoshmërisht pasqyrojnë pikëpamjet dhe mendimet e Çështjeve Globale të Kanadës, Qeverisë të Kanadës, Qeverisë të MB, USAID-it apo Qeverisë të Shteteve të Bashkuara.

Fotografia e kopertinës: Brett Sayles (Pexels)

Tabela e Përmbajtjes

Fondacioni Ndërkombëtar për Sistemet Zgjedhore

Përmbledhja ekzekutive

Shoqëritë gjithnjnë e më shumë mbështeten në teknologji nëpër sektorë të ndryshëm pasi gjithnjë e më shumë procese transaksionale po digjtalizohen. Rasti i njëjtë po ndodh edhe me zgjedhjet, ku kompjuterët dhe teknologjia janë bërë të domosdoshme për sjelljen e tyre. Pandemia COVID-19 që po ndodh aktualisht ka rritur interesin dhe kërkesën për të lëvizur shërbimet në largësi, në hapësira elektronike. Dhe kjo kërkesë po rritet, marrësit e vendimeve zgjedhore duhet të njohin natyrën e veçantë të proceseve zgjedhore dhe duhet të marrin parasysh faktorët e rëndësishëm të rrezikut kur konsiderohet përdorimi i votimit përmes internetit.

Sot, shumica e organeve për menaxhimin e zgjedhjeve (OMZ) përdorin një shkallë të teknologjisë për të përmirësuar proceset zgjedhore. Nga mjetet standarde të zyrës dhe faqet themelore të internetit deri në bazat e sofistikuara biometrike të të dhënave të listës zgjedhore dhe sistemet tërësisht elektronike në internet për votim, teknologjitë e reja mund të premtojnë mundësi të reja për të ofruar zgjedhje më efikase, të sakta dhe mundësisht më transparente. Ata gjithashtu sjellin rreziqe të reja: Teknologjia që nuk është pjekur, dobët e planifikuar që funksionon në mënyrë të pasaktë nga përdorues jo të trajnuar apo krijon mundësi të reja për aktorët me qëllime të këqija që të ndërhyjnë në sigurinë dhe integritetin e proceseve zgjedhore mund të minojnë besueshmërinë e qytetarëve.

Prezantimi i votimit përmes internet – në mënyrë specifike, përdorimi i internetit për të votuar me fletëvotimin jashtë vendvotimit – është ndoshta mbindërtimi më i vështirë teknologjik për një OMZ, sepse prek mbi thelbin e procesit zgjedhor. Votimi në largësi përmes internetit në masë të madhe zvogëlon kontrollin e drejtëpërdrejtë të zyrtarëve zgjedhor mbi procesin zgjedhorë. Siguron mundësinë për të zgjidhur disa problem historike – siç është fuqizimi i të drejtës të votuesve jashtë shtetit, votuesve me aftësi të kufizuara dhe personat e shpërngulur brenda shtetit – dhe paraqet një mundësi që mundësisht të merren rezultate të shpejta pa gabime që shkaktohen nga njërëzit për shembull gjatë numërimit. Megjithatë, gjithashtu prezanton një varg të gjërë të rreziqeve dhe shqetësimeve nga perspektiva e sigurisë, fshehtësisë të votimit, transparencës dhe besimit. Si pasojë, diskutimi i votimit përmes internetit zakonisht nxit më shumë kritika dhe është kontestuar më shumë se sa përdorimi i çfarëdo teknologjie tjetër në zgjedhje. Votimi përmes internetit akoma është një teknologji në zhvillim, me vetëm disa raste të suksesit nga të cilat mund të studiojmë dhe mësojmë.

Duhet të vlerësohet rëndësia e kësaj teknologjie para se të zbatohet në çfarëdo konteksti sipas pesë parametrave: kostoja, pjesëmarrja, efikasiteti, besimi dhe siguria. Siguria i referohet jo vetëm mundësisë për sulme kibernetike, për shembull, por edhe sigurisë personale – dmth, privatësisë personale dhe fshehtësisë të nevojshme për të votuar me fletëvotimin e ndonjë personi.

Përderisa **kostoja e votimit përmes internetit** përfundimisht mund të bëhet më e ulët se e votimit tradicional, kjo do të marrë disa cikle zgjedhore që të arrihet sepse fillimi i këtij sistemit kërkon një prokurim respektivisht furnizim të ri domethënës, trajnim, fushata për vetëdije publike dhe siguri të përfshirë. Votimi përmes internetit shpeshherë mbështetet në kostot e pallogaritura siç janë infrastruktura e fuqishme e identifikimit – kartelat biometrike të votimit, kartelat e mençura të identifikmit, ejt. – që mund të jenë shtrenjtë nëse akoma nuk janë në vend.

Përderisa votimi përmes internetit mund të duket tërheqës për të rritur daljen e votuesve, studimet kanë treguar se kjo nuk ndodhe në përgjithësi. Ky studim ka gjetur se **votimi përmes internetit mund ta bëjë votimin "më të përshtatshëm" për votuesit ekzistues, por nuk ka tendencë që të tërheq votues të ri.** Votuesit e rinj në veçanti, duket se më shumë shqetësohen për atë se pse duhet të votojnë, e jo se si të votojnë.

Shumica e formave të votimit elektronik, duke përfshirë edhe votimin përmes internetit e përmirësojnë shpejtësinë dhe besueshmërinë e votimit. Votimi përmes internetit mund të jetë përfitues për një grupë të madhe të njerëzve që të ushtrojnë të drejtën e tyre, siç janë votuesit që nuk kanë mundësi të votojnë deri te vendovotimet e tyre apo votuesit me aftësi të kufizuara. Megjithatë, në të njëjtën kohë, votimi përmes internetit mund të përjashtojë komunitetet tjera – ata që ose nuk kanë qasje në internet apo nuk dijnë të përdorin internetin, duke ndikuar shumë raste në mënyrë disproporcionale në votuesit me moshë të vjetër dhe që jetojnë në vendbaanime rurale. Nëse realizohet, do të ketë nevojë për një edukim të gjërë dhe të fuqishëm të votuesve.

Teknologjia që mbështet votimin përmes internetit është shumë e sofistikuar, duke përfshirë matematikë dhe kriptografi të sofistikuar. Shumë prej votuesve nuk do të kuptojnë si funksionon, dhe kjo mungesë e të kuptuarit mund të minojë **besimin publik.** Ky besim mund të fitohet duke vendosur procedura të hollësishme, duke përfshirë rishikimin (auditimin), dhe të sigurojë palët e interesuar me informacione të mjaftueshme që të kuptojnë plotësisht sekuencën dhe mekanizmat e procesit të votimit. Duhet të kemi kujdesin e duhur në lidhje me pikëpamjet e qytetarëve. Një mungesë e besimit në procesin zgjedhor mund të ndikojë në mënyrë dramatike legjimitetin e perceptuar të atyre që janë zgjedhur.

Siguria–si dhe perceptimi i sigurisë – duhet të jetë konsiderata kryesore para realizimit të votimit përmes internetit. Disa shtete janë larguar nga progamet e kufizuara të votimit përmes internetit – duke përfshirë Francën, Hollandën dhe Norvegjinë– për shqetësimet e sigurisë. Shtetet të cilët përjetojnë sulme kibernetike të shpeshta e ndonjëherë shkatërruese duhet të ndërmarrin të gjithë masat e nevojshme për të rritur rezistencën e infrastrukturës të tyre zgjedhore. Siguria personale meqënëse lidhet me privatësinë e votuesit, gjithashtu duhet të merret parasysh. Me votimin në distancë përmes internetit, duhet të ndërmerren masa për të siguruar se është siguruar dhe zbatuar fshehtësia e votës.

Teknologjitë mund të përforcojnë proceset zgjedhore nëse konsiderohen dhe zbatohen me sukses; ky proces nuk duhet të përshpejtohet për shkak të pasojave shumë të mëdha në rast të dështimit. Faza e parë në procesin e të menduarit të miratimit të votimit elektronik dhe teknologjive të numërimit është një studim i fuqishëm i fizibilitetit dhe testimit të teknologjisë së re në numër të vogël të konstituentëve, para se të vendoset në shkallë në zgjedhje të detyrueshme

Hyrje

Meqënëse teknologjia po avancon dhe shumë transaksione po bëhen në formën elektronike, shumë njerëz pyesin se kur votimi do të hyjë me të vërtetë në epokën digjitale. Në fund të fundit, shumë përdorues të internetit u besojnë faqeve të internetit dhe aplikacioneve ne telefon mobil informacione financiare dhe bashkëveprime sociale – duke se është e natyrshme të kemi nivelin e njëjtë të besimit kur votojmë respektivisht hedhim votën në formë elektronike (online).

Gjatë pandemisë COVID-18, të gjitha bizneset, vendet e punës, zyrat qeveritare dhe shërbimet arsimore me shpejtësi kaluan në internet. Megjithatë, zgjedhjet kanë karakteristika të veçanta. Ka shumë çështje komplekse, serioze për të marrë në konsideratë kur flasim për votimin përmes kompjuterit apo telefonit në një mjedis të pakontrolluar – keto çështje ndikojnë në mënyrë thelbësore në legjitimitetin e perceptuar të atyre që janë zgjedhur, dhe vetë integritetin e demokracisë. Këto çështje përfshijnë besimin e publikut, fshehtësinë e fletëvotimit, shtrëngimin, frikësimin dhe mekanizmat e besueshme të identifikimit. Një sistem që duhet të jetë tërësisht i verifikueshëm për të siguruar se të gjithë votat janë dhënë ashtu siç janë planifikuar dhe janë përmbledhur ashtu siç janë votuar pa rrezikuar fshehtësinë e fletëvotimit.

Ky dokument nuk synon që të theksojë nëse votimi përmes internetit duhet të përdoret apo shmanget: Fondacioni Ndërkombëtar për Sistemet Zgjedhore (IFES) nuk është në mënyrë univerzale për ose kundër votimit përmes internetit. Përkundrazi, duke siguruar një shqyrtim të rasteve studimore dhe literaturës ekzistuese, ky studim synon që të ndihmojë palët e përfshira në zgjedhje në bërjen e pyetjeve të duhura për të identifikuar nëse votimi përmes internetit do të përmirësojë më tutje integritetin zgjedhor dhe demokracinë, apo nëse do të minonte besimin publik dhe sigurinë e procesit zgjedhor.

Historia dhe përdorimi i votimit përmes internetit

Përderisa votimi përmes internet për votimin në distancë ka potencial në të ardhmen, është një qasje e re që është zbatuar me sukses vetëm në disa raste. Votimi përmes internet është ende një teknologji në zhvillim kur bëhet fjalë për sigurinë dhe besimin; shumë shtete kanë zgjedhur të mos përdorin atë pasi kanë kryer studimet e fizibilitetit apo pilotimet për shkak të shqetësimeve të sigurisë. Votimi përmes internetit është përdorur për herë të parë për zgjedhjet politike të detyrueshme në vitin 2000 në Shtetet e Bashkuara të Amerikës (SHBA) në një pilot në disa shtete që synonin votuesit jashtë shtetit. Që atëherë, afërsisht dymbëdhjetë shtete kanë ekperimentuar më këtë teknologji. Ky studim nuk shqyrton përdorimin e votimit përmes internetit në mjedise të kontrolluara, siç janë vendvotimet, sepse kjo është e ngjajshme me disa metoda tjera të votimit elektronik mbi të cilat tashmë ka një hulumtim domethënës.

Estonia është shteti i vetëm që përdor votimin përmes internetit në të gjithë shtetin. Disa shtete të tjera e përdorin votimin përmes internetit në disa pjesë të shtetit apo për anëtarë të caktuar të elektoratit (Armenia, Australia, Kanada, Panama, Zvicra dhe SHBA). Disa shtete kanë bërë pilotime të kufizuara të votimit përmes internetit dhe kanë vendosur të mos vazhdojnë përdorimin e tij (Mbretëria e Bashkuar dhe Norvegjia). Shtetet tjera në fillim miratuan votimin përmes internetit por vendosën që të mos e vazhdojnë atë (India, Franca, Hollanda dhe Spanja).[1] Shihni Aneksin 2 për më shumë informacion për atë se si shtetet individuale kanë përdorur apo pilotuar votimin përmes internetit. Shtetet që përdorin votimin përmes internetit kanë tendencë të synojnë kategori specifike të votuesve – për shembull, votuesi jashtë shtetit, personelin diplomatik apo ushtarak jashtë shtetit, votuesit që mungojnë apo votuesit me aftësi të kufizuara. Në përgjithësi, votimi përmes internetit është ofruar për votuesit para Ditës të Votimit për një periudhë që ndryshon nga shteti në shtet por zakonisht përfshin ndërmjet një dhe dy javëve.

Analiza tematike

Për të vlerësuar nëse votimi përmes internetit është i duhuri, shteti duhet të kryejë një studim të fizibilitetit që analizon se si ky ndyshim ndikon në aspektet kritike të procesit demokratik. Ky studim duhet që në mënyrë specifike të fokusohet në çështjet që shteti përpiqet të rregullojë ose përmirësojë duke zbatuar këtë teknologji: psh: kostoja apo dalja e votuesve. Në përgjithësi, teknologjia duhet vetëm të prezantohet si "zgjidhje" nëse ka ndonjë problem për të cilin mund të ndihmojë që ta lehtësojë. Përderisa Estonia shfrytëzon votimin përmes internetit në të gjithë shtetin, ka shumë arsye serioze tjera që shtetet tjera kanë zgjedhur për të mos e zbatuar këtë mekanizëm. Çfarëdo vendimi nuk duhet të shoh vetëm në teknologjinë që do të kërkohet, por edhe anët pozitive dhe negative që zbatimi do të ketë mbi elektoratin dhe integritetin e procesit zgjedhor. Mundësitë – dhe rreziqet – e kësaj teknologjie duhet të vlerësohen para se të zbatohet në çfarëdo konteksti sipas pesë parametrave: kostoja, pjesëmarrja, efikasiteti, besimi dhe siguria.

[1] Më shumë detaje dhe një listë të përditësuar të shteteve dhe modelet e zbatimit janë të disponueshme në Aneksin 2

Kostoja

Zgjedhjet shpesh konsiderohen sfida më madhe logjistike me të cilën përballet një shtet gjatë kohës të paqes. Kostoja e përgjithshme e zgjedhjeve është e vështirë që të llogaritet sepse shpesh përdoret infrastruktura publike për të mbështetur funksionimin gjatë Ditës të Votimi dhe procesit të numërimit. Për shkak të kësaj kostoje të lartë logjistike dhe përdorimit të infrastrukturës, idea e digjitalizimit të operacioneve zgjedhore është tërheqëse. Kursimi i kostos në fakt mund të paraqitet në afat të gjatë, duke supozuar se, nëse dalja e votuesve mbetet konstante, numri votuesve përmes internetit rritet dhe numri i votuesve tradicional zvogëlohet. [2] Megjithatë, nuk ka gjasa që votimi përmes internetit do të zvogëlojë kostot e njësive që përndryshe janë të shtrenjta, siç janë lista zgjedhore, përcaktimi i kufijve dhe emërimi i kandidatëve. Përveç asaj, ka gjasa që votimi në distancë përmes internetit të mos jetë mundësia e vetme e votimit në dispozicion për një ose dy ciklet e para, që do të thotë se administratat zgjedhore do të duhet të ofrojnë votimin me personat fizikisht të pranishëm dhe votimin përmes internetit, dhe rrjedhimisht të shohim rritje në vend se zvogëlim të kostove në afatin e shkurtër ose të mesëm.

Mësime nga Estonia

Programi i kartës të programit të ID të Estonisë dhe sistemi i votimit elektronik nuk ka qënë pa polemika.

Një rishikim i botuar në vitin 2014 nga një ekip i studiuesve ndërkombëtar kanë kritikuar sigurinë e dobët operative dhe procedurale. Ai ka demonstruar rrezikshmëritë kryesore që ka mundësi të shfrytëzohen për të prishur votat dhe për të marrë kontrollin e serverëve.

Një rrezikshmëri kritike e identifikuar në vitin 2017 në sistemin e kartës të ID, duke lejuar secilin që di çelësin publik të kartës të ID për të kopjuar çelësin privat për një kosto relativisht të ulët dhe të përdoret për të kontrolluar në tërësi identitetin e personit pa poseduar kartën fizike të ID. Ndikimi i kësaj rrezikshmërie në procesin zgjedhor mund të ketë qënë jashtëzakonisht i dëmshëm nëse koha e zbulimit do të ishte e ndryshme. Autoritetet e Estonisë janë rikuperuar nga kriza me miratimin e politikës të transparencës maksimale për ndikimim e rrezikshmërisë dhe veprimit që ata merrnin për të zbutuar atë. Kjo është e mundur vetëm në kontekstin ku qytetarët i besojnë autoriteteve dhe ku popullsia është relativisht e vogël dhe homogjene – Estonia kishte 887,420 persona me të drejtë vote në vitin 2019.

Disa studime dhe publikime demonstrojnë se kostoja e votimit përmes internet është shumë më e ulët se votimi standard – afërsisht gjysma. Megjithatë, *ata nuk llogarisin kostot e trajnimit dhe ushtrimet për vetëdijen publike as edhe kostot për vendosjen e një infrastrukture të besueshme elektronike të identitetit,* si ajo në të cilën mbështetet sistemi i votimit përmes internetit në Estoni.

Sistemi i votimit përmes internetit në Estoni është ndërtuar duke marrë për bazë kartën ID të Estonisë. Rrjedhimisht, nuk është e mundur që të ndahet në mënyë të arsyeshme kostoja e votimit përmes internetit nga dekadat e investimeve në shkallë të madhe në ekosistemin e e-qeverisjes që përfshin të dhënat sistemin e të dhënave të ndër-agjencive (X-rrugëet), një dokument ID të detyrueshëm elektronik (që të dyja qeveria Estoneze ka zhvilluar që nga viti 1990) dhe sigurimi votimit përmes internetit (eesti.ee)[3].

[2] Fondacioni Ndërkombëtarë për Sistemet Zgjedhore, Ben Goldsmith, *Votimi përmes Internetit:E kaluara, e tashmja dhe e ardhmja,2013*; https://www.ifes.org/news/Internet-voting-past-present-and-future

[3] Estoniaka bërë një investim thelbësor në ekosistemin e –qeverisjes të tyre, kostoja e plotë e të cilit është e vështirë për ta vlerësuar dhe nuk është publikisht e disponueshme. Disa vlerësime thonë që mirëmbajtja vetëm e x-rrugëve është 50 deri në 60

Karta e Estonisë është një ID nacional i detyrueshëm, që është një kartë e mençur që lejon një vertetim të sigurtë në distancë dhe ligjërisht të detyrueshëm të nënshkrimeve digjitale për përdorim në infrastrukturën kryesore publike mbështetur nga shteti i Estonisë[4]. Kartelat e mençura janë prezantuar në vitin 2002 dhe shërbimet janë zgjeruar në mënyrë progresive gjatë viteve. Kjo infrastrukturë mund të përdoret për identifikim dhe vërtetim për të gjithë shërbimet qeveritare, siç janë deklarimet tatimore, dëshmi të identitetit për qasje në llogaritë bankare, të kontrollohen të dhënat mjekësore dhe përdorimi i e-udhëzimeve dhe më tepër. Ka patur kritika gjatë rishikimit[5] dhe zbulimit të rrezikshmërive[6](shihni mësime nga Estonia" në tekstin më poshtë)[7]. Në Estoni, votuesit e vërtetojnë veten e tyre në një faqe internet për të dhënë votën e tyre elektronike. Ata përdorin një harduer shtesë: lexuesi i kartelës ID, të lidhur me kompjuterin e tyre, që lexon çelësin e enkriptuar në kartelë. Votuesit mund të ndrrojnë votën e tyre sa here të duan, me votën e tyre të fundit që është përfundimtare ajo që është përmbledhur. Gjithashtu është e mundur për secilin që voton përmes internetit të votojë në vendvotim gjatë periudhës të votimit të hershëm, duke e bërë të pavlefshme në mënyrë automatike votën e tyre përmes internetit, por kërkon që vendvotime që mund të pështasin votuesit nëse ata kanë votuar në formë elektronike apo jo.

Kështu, përderisa llogaritë fillestare të kostos mund të duket se janë në favor të votimit përmes internetit në horizontet afatshkurta, faktorizimi i kostove afatmesme dhe afatgjata që nuk janë menjëherë intuitive mund të sjellin në një llogaritje shumë të ndryshme të kostos. Është detyrim që kjo të ndodhë në fillim

Mësime nga Norvegjia

Norvegjia ka pilotuar një sistem të kufizuar të votimit përmes internetit për zgjedhjet komunale në vitin 2011 dhe 2013, por ka anulluar projektin në vitin 2014, duke theksuar shqetësimet e sigurisë dhe përfundimin e qeverisë se, përkundër pritshmërive, sistemi i ri nuk e ka përmirësuar daljen në votime. Instituti norvegjez i Hulumtimi Social ka thënë se "*se nuk ka dëshmi se prova ka sjelluar rritje të numrit të përgjithshëm të personave që votojnë, e as që ka mobilizuar grupe të reja të votojnë, siç janë personat e rinj që të votojnë." Edhe vetëm një përmbledhje e përpjekjeve të ulëta"të sistemit nga ekspertët kompjuterik nga Qendra Norvegjeze kompjuterik dhe Universiteti Norvegjez i Shkencave dhe Teknologjisë kanë gjetur "problemet domethënëse" me sigurinë, ndër të tjera, në masën sa ekspertët thanë se softueri "nuk kishte cilësinë e pranushme për përdorim në sistemin e e-votimit*."Është me rëndësi të theksohet se autoritetet norvegjeze nuk kanë përmendur sigurinë si një shqetësim kryesor, në kundërshtim e me shumicën e vlerësimeve tjera dhe rasteve studimore. Megjithatë, është raportuar se votuesit kanë njohuri shumë të kufizuar për mekanizmat e sigurisë në sistem, që ndikojnë në premise për zgjedhje të lira dhe të drejta.

milion dollarë amerikanë në vjet https://www.innovations.harvard.edu/blog/estonia-one-small-country-digital-government-having-big-impact-x-road

[4] Robert Krimmer, David Duenas-Cid dhe Iuliia Krivonosova (2020) *Metodologjia e re për llogaritjen e efikasitetit të kostos të mënyrave të ndryshme të votimit: a është votimi me internet më i lirë?*, Paratë Publike dhe Menaxhimi: https://www.tandfonline.com/doi/full/10.1080/09540962.2020.1732027

[5] Shqyrtimi i botimit zyrtar dhe përgjigja për identifikimin e gabimit ROCA në kartën e ID të Estonisë; https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf dhe https://e-estonia.com/wp-content/uploads/faq-a4-v02-id-card-1.pdf)

[6] Prezantimi i auditit nga ekipi ndërkombëtar; https://estoniaevoting.org/ dhe https://nordicinnovationla bs.com/wp-content/uploads/2018/07/ivoting-ccs14.pdf;përgjigje nga Komisioni Zgjedhor i Estonisë;https://estoniaevoting.org/press-release/response- national-election-committees-statement/

[7] Rekomandime nga Raporti Përfundimtar i OSBE/ODIHR për Zgjedhjet Parlamentare në Estoni, 2005-2019.

të diskutimit ashtuqë palët e përfshira të kuptojnë në tërësi kriteret mbi të cilat ata mbështesin vendimin nëse do të ketë apo jo zbatim të asaj teknologjie.

Ndikimi mbi daljen e votuesve

Dalja në votime në ngjarjet zgjedhore po zvogëlohet në të gjithë botën. Shumë qeveri po kërkojnë mënyra për të përmirësuar sistemet e votimit tradicional për të kundërshtuar atë që e perceptojnë si kërcënim të shkaktuar nga rënia e pjesëmarrjes demokratike. Votimi përmes internetit mund të duket si përgjigje e arsyeshme për këto shqetësime, sidomos duke konsideruar lehtësimin e mundshëm të faktorëve të kursimit - të qasjes dhe kohës për disa votues. Ka shumë studime që supozojnë se të siguruarit e kanaleve të ndryshme të votimit e rrit daljen e votuesve. Për fat të keq, këto studime janë zakonisht shumë partiake, duke konsideruar vetëm përfitimet që teknologjia mund të sjell, ndërsa kryesisht mbështeten në hipoteza dhe në anketa të opinioneve sesa në hulumtime të bazuara në dëshmi. Shpesh këto studime bëjnë përfundime të gjëra pa parë në kontekstin specifik politik apo të shtetit, implikimet shoqërore apo faktorë tjerë që përcaktojnë daljen e votuesve: psh., mungesa e besimit në sistem, të qënit të kënaqur me gjendjen e pandryshueshme (status quo), lloji apo niveli i zgjedhjeve, besimi në parti dhe kandidatë, intensiteti i fushatës dhe interesi i medias në zgjedhje.

Pandemia e COVID-19 paraqet një situatë të paprecedentë për botën moderne, me qytetarë në shumë shtete që nuk kanë mundësi të votojnë apo të lënë shtëpitë e tyre. Një sistem i votimit elektronik në distancë mund të zgjidh disa nga pengesat në pjesëmarrje nëse për shembull, numër i madh i elektoratit nuk kishin mundësi që të udhëtojnë fizikisht në vendvotim për shkak të një emergjence të papritur kombëtare (apo, në këtë rast, globale). Megjithatë, një sistem që shfrytëzon, votimi elektronik në distancë merr një kohë të gjatë për të qënë i vendosur në mënyrë efektive. Nëse tashmë është në vend dhe i testuar para emergjencës, kjo mund të jetë pozitive në aspekt të daljes të votuesve gjatë krizës si COVID-19. Megjithatë, për shkak të niveleve të larta të planifikimit, përgatitjes dhe testimit të nevojshëm, nuk ka gjasa që shtetet që nuk kanë një sistem në vend do të kenë mundësi – apo duhet që të përpiqen – të fillojnë votimin përmes internetit si një përgjigje të menjëhershme ndaj një krize.

Duke qënë shteti i vetëm që zbaton votim përmes internetit në të gjithë shtetin, Estonia mundet sërisht që të sigurojë disa të dhëna dhe informacione sasiore.[8] Në Estoni, nuk kishte një ndryshim domethënës në pjesëmarrjen e votuesve pas prezatimit të votimit përmes internetit; është vëzhguar si të jetë një mekanizëm votimi zëvendësues për votuesit tashmë të angazhuar në procesin zgjedhor.[9] Ndërmarrja kryesore në aspekt të përvojës të votuesit është se e bën votimin më të "përshtatshëm" për votuesit ekzistues, në vend se të rrisë pjesëmarrjen e atyre të cilët nuk kanë votuar më parë.[10] Tendenca po

[8] Tove Wigartz (Universiteti i Gotenburgut), *A ndikon votimi përmes internetit në daljen e votuesve në Estoni?, 2017*; https://core.ac.uk/download/pdf/95665595.pdf

[9] Kitsing Meelis, *Pjesëmarrja elektronike në Estoni: Votimi aktiv, angazhimi i ulët*, *2011*; https://www.researchgate.net/publication/221547555_Online_participation_in_Estonia_Active_voting_low_engagement

[10] Referenca tjera për ndikimin e votimit përmes internetit në daljen e votuesve në Estoni; http://www.democraticaudit.com/2013/10/03/the-estonian-experience-shows-that-while-online-voting-is-faster-and-cheaper-it-hasnt-increased-turn-out/; një shqyrtim i statistikave të votimit përmes internetit të menaxhuara nga qeveria e Estonisë; https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia

tregon se gjithnjë e më shumë njerëz votojnë në formë elektronike, dhe se votuesit që kanë votuar në formë elektronike do të vazhdojnë ta bëjnë atë. Shembulli norvegjez shton një gjetje interesante në lidhje me votuesit e rinj, të cilët shpesh janë përdor si një argument në dobi të votimit përmes internetit. Votuesit e rinj që marrin pjesë në zgjedhjet pilotuese në Norvegji duket se preferojnë që të votojnë në vendvotimet e tyre në Ditën e Votimit si një deklaratë politike. Duke u bazuar në gjetjet nga komisioni që analizon rezultatin e pilotimit, personat e rinj kanë raportuar se janë më të shqetësuar për pyetjen se pse personat e rinj duhet të votojnë në vend se si do të votojnë.[11]Përdesa votimi përmes internetit nuk duhet të përjashtohet në aspekt të mundësisë të tij për rritjes të pjesëmarrjes të votuesve, kjo duhet të shoqërohet me një edukim të gjërë qytetarë dhe të votuesve dhe informacione publike që do të inkurajojnë votuesit të marrin pjesë në procesin politik.

Qasshmëria

E drejta në votë për përfaqësuesit e zgjedhur është një gur themel i demokracisë, i mbrojtur nga disa përkushtime ndërkombëtare duke përfshirë Dokumentin e Kopenhagës dhe Konventën e Kombeve të Bashkuara mbi të Drejtat e Personave me Aftësi të Kufizuara. Megjithatë, për votuesit me aftësi të kufizuara vendvotimet e të cilëve nuk janë të qasshme, kjo e drejtë nuk është respektuar në masë të madhe në shumë shtete reth botës. Votimi përmes internetit mund të sigurojë mundësinë për më shumë njerëz me aftësi të kufizuara të kenë qasje në të drejtën e tyre të japin votën nëse nuk ka opsione tjera të disponueshme të votimit në distancë. Përveç asaj, aftësia e votuesit me aftësi të kufizuara për të përdorur pajisjen e tij elektronike për të votuar mund të sigurojë më shumë lehtësi në qasje, sepse shumë pajisje përfshijnë funksionet e qasshmërisë që sigurojnë opsione të ndryshme psh. audio apo tekst të madh. Megjithatë edhepse, votimi në distancë përmes internetit siguron disa lehtësira për personat me aftësi të kufizuara, duhet të jetë bashkë me një listë zgjedhore të qasshme dhe procese të identifikimit, si dhe informim dhe edukim të votuesve në forma që janë të qasshme dhe të lehta për të kuptuar nga të gjithë votuesit, duke përfshirë edhe votuesit me aftësi të kufizuara.

Efikasiteti

Votimi përmes internetit mund të bëjë procesin e votimit dukshëm më të shpejtë për votuesit që kanë mundësi ta përdorin atë, duke kursyer kohën dhe ndoshta edhe pengasat fizike që përfshijnë udhëtimin deri dhe nga vendvotimi, duke shmangur radhët e mundshme dhe duke iu lejuar votuesve të votojnë shpejtë nga shtëpia e tyre. Megjithatë është me rëndësi të theksohet se jo të gjithë votuesit janë domosdoshmërisht të përshtatshëm me kompjuterë apo teknologji; sidomos duhet të ushtrohet kujdes i veçanteë për të kuptuar nivelin e edukimit teknologjik në vend. Gjithashtu duhet kushtuar vëmendje infrastrukturës, në aspekt të niveleve të internetit publikisht të disponueshëm si dhe infrastrukturën personale – nëse personat kanë apo jo telefona mobil me internet të mjaftueshëm, nëse kanë kompjuterët me gjërësi të mjaftueshme të shtritjes të valëve të internetit, etj.

Përderisa rezultatet dhe vetë votimi janë më të shpejtë përmes votimit elektronik, është me rëndësi të

[11] Studimi i ndikimit të votimit përmes internetit në Norvegji; https://www.regjeringen.no/en/historical- archive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regiona/tema-og-redaksjonelt- innhold/kampanjesider/e-vote-trial/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trials-in- 201/summary-of-the-isf-report/id685824/

konsiderohet se çfarë sakrifikohet për këtë menjëhershmëri dhe komoditet dhe çfarë hapash duhet të merren për ta zbutur atë. Në aspekt të kohës – dhe legalitetit, marrësit e vendimeve gjithashtu duhet të konsiderojnë se çfarë ndryshimesh ligjore janë të nevojshme për të prezantuar votimin në distancë përmes internetit si një opsion.[12] Në varësi nga konteksti, ky proces i ndryshimeve mund të jetë i gjatë dhe të marrë kohë domethënëse. Kondideratat ligjore duhet të përfshijnë këto kategori:

- Fshehtësia e votës: një nga çështjet më kundërshtuese është nëse votimi në mjedise të pakontrolluara është konsistente me parimin e të drejtës në votë në fshehtësi, dhe si fshehtësia e votës mund të sigurohet kur një votë është dhënë në distancë në një pajisje personale.[13]
- Rishikimet, rinumërimet dhe administrata: Konsiderata duhet të jepen për kornizën ligjore që rregullon rishikimin dhe administrimin e zgjedhjeve dhe kompetencën e administratorëve zgjedhorë, duke përfshirë certifikimin e sistemeve, rishikimet, rinumërimet, gjurmimi i rishikimit të vërtetimit të votuesi dhe më shumë.
- Efekti mbi kërksat e transparences, siç është roli i vëzhguesve edhe agjentëve partiak
- Ndikimi i votimit përmes internetit mbi votat jo të vlefshme dhe të zbrazëta

Më në fund, prezantimi i e-votimit kërkon ndryshime thelbësore në kornizën nacionale ligjore që rregullon zgjedhjet. [14] Megjithatë, projektet fillestare pilotuese mund të kërkojnë dispozita të veçanta në lidhje me këto projekte eksperimentale para se të zbatohet rishikimi i përgjithshëm të kornizës ligjore, nëse një votim i tillë do të prezantohet në të gjithë shtetin.

Sistemi i kontrollit të votimit elektronik

Sistemi i kontrollit të votimit elektronik (SKTE) është një kërkesë për secilin sistem të besueshëm të e-votimit. Pa të, nuk ka mënyrë për të siguruar besim në proces dhe për rishikim të fletëvotimit. Ky sistem përdor funksione kriptografike për të lejuar votuesin të vërtetojë respektivisht të kontrollojë nëse fletëvotimi është hedhur siç është destinuar (regjistruar) dhe është përmbledhur(numëruar) siç është votuar (kontroll individual). Ky sistem gjithashtu u lejon palëve të treta të kontrollojnë rezultatin për të konfirmuar se është i saktë (kontrollimi universal). Kjo mundëson që të mund të bëhet rishikimi i saktësisë të rezultatit, sipas mundësisë nga të gjithë palët e përfshira: organizatat individuale ose të pavarura, siç janë mediat, partitë politike, organizatat joqeveritare. Ashtu si edhe gjithë sistemet tjera në internet, ky sistem (SKTE) nuk mbron nga programet me qëllime të këqija të cila mund të jenë

[12] Ka disa referenca ndërkombëtare që mund të rishikohen kur mendoni për ndryshime në kornizën ligjore. Raporti i IFES mbi votimin përmes internetit në Norvegji ka siguruar një kornizë për të kontrolluar harmonizmin e votimit përmes internetit me standardet ndërkombëtare: https://www.regjeringen.no/globalassets/upload/krd/prosjekter/e- valg/evaluering/topic7_assessment.pdf. Rekomandimet e Këshillit të Europës të vitit 2017 janë ndoshta standardet më të rëndësishme deri sot, me më shumë se 49 pikë të grupuara nga *E drejta univerzale në votë, e drejta e barabartë në votë, e drejta në votë të lirë, e drejta në votë të fshehtë , Kërkesat rregullative dhe organizative, transparenca dhe vëzhgimi, llogaridhënia dhe besueshmëria, dhe siguria e sistemit:* https://www.coe.int/en/web/electoral-assistance/-/council-of-europe-adopts-new-recommendation-on- standards-for-e-voting. Gjithashtu ka një organ në zhvillim të standardeve tjera të votimit elektronik nga IFES, OSBE/ODIHR, Qendra Karter dhe të tjerët, sidomos në lidhje me vëzhgimin e zgjedhjeve por gjithashtu e zbatueshme si udhëzime për OMZ.

[13] Ky diskutim gjithashtu ka të bëjë me votimin përmes postës dhe mundësinë që votuesit të votojnë disa herë. Estonia, që është diskutuar më poshtë, e zbut këtë dhe shtrëngimin e mundshëm duke numëruar vetëm fletëvotimin e fundit elektronik të dhënë nga votuesit. Në Estoni, gjithashtu është e mundur për secilin që ka votuar përmes internetit të jap votën e tij në vendvotim në Ditën e Votimit, dhe kjo e anulon votën e tij apo saj të dhënë përmes internetit.

[14] Kodi i Praktikave të Mira në Çështjet Zgjedhore i Komisionit të Venedikut thekson se nuk duhet të bëhen ndryshime të mëdha në legjislacioni zgjedhor brenda vitit, para ngjarjes të zgjedhjeve;https://rm.coe.int/090000168092af01

dizajnuar në mënyrë specifike për spiunuar përzgjedhjen e e votuesit, të kompromentojë fshehtësinë e fletëvotimi, ose të votohet përmes mashtrimit në emër të votuesit.

Për më tepër, është e vështirë që të sigurohet një mënyrë për votuesit që të mund të kontrollojnë se si kanë votuar pa e bërë gjithashtu të mundur për votuesit që të mund të dëshmojnë para një palë të tretë se si kanë votuar, që paraqet rrezikun e blerjes të votës apo shtrëngimit. Gjatë viteve, Estonia ka përmirësuar teknikat për të lejuar votuesit që të kontrollojnë votën e tyre para se ajo të regjistrohet për gjithmonë. Pasi të jepet vota me fletëvotim përmes kompjuterit, secili votues pranon një kod QR që është i vlefshëm vetëm për 30 minuta dhe i lejon votuesit që të kontrollojë votën nga një pajisje e ndryshme: p.sh., një telefon i mençur.[15]Kjo, sigurisht që mbështetet në faktin që votuesi ka disa pajisje të lidhura me internet. Vini re se kontrollimi i pronës të këtij sistemi (SKTE) në votimin përmes internetit gjithashtu krijon rrezikun për blerje të votës, dhe aktualisht nuk ka ndonjë teknologji për ta zbutur respektivisht lehtësuar një gjë të tillës.

Aftësia e kufizuar për të rishikuar rezultatet

Rishikimet për të kufizuar rrezikun, si dhe aftësinë për të kryer çfarëdo llojë të rinumërimit, është shumë të kufizuara për të mos thënë e pamundur kur votohet në mënyrë elektronike. Për dallim nga disa pajisje moderne të votimit elektronik, këtu nuk ka gjurmë të rishikimit të letrës. Kjo e bën më të vështirë për OMZ për të rishikuar rezultatet nëse ka ndonjë mosmarrëveshje. Në një mjedis politik dhe social që kërkon besim dhe transparencë, kjo është ndoshta mangësia e vetme më e rëndësishme e votimit përmes internetit.

Një rrezik që kufizon rishikimin pas zgjedhejve kërkon kontrollimin me dorë të një shembulli të rastisshëm që është statikisht i rëndësishëm të fletëvotimit në letër për të pare nëse pajiset e votimit elektronik dhe skanerët e fletëvotimeve i kanë interpretuar ata siç duhet.[16]Një rishikim i krahahasuar i fletëvotimit kërkon një numërim të pavarur të gjithë fletëvotimet e kompjuterëve, jo vetëm shembullin, për të kontrolluar nëse kompjuterët e zgjedhjeve kanë bërë përmbledhjen përfundimtare në mënyrë të saktë. Rishikimet pas zgjedhjeve janë parësore për zgjedhjet me numërim elektronik të votave dhe janë pjesë e praktikës të mirë në të gjithë botën. [17] Përfitimet e tyre janë vlerësuar nga ata që merren me shkenca politike, ekspertët e statistikave dhe sigurisë të zgjedhjeve. [18]

Besimi dhe transparenca

Proceset e sistemeve zgjedhore duhet të ofrojnë respektivisht japin rezultate që pasqyrojnë vullnetin e votuesve në një mjedis që krijon një besim të mjaftueshëm ashtuqë këto rezultate pranohen si të vlefshme. Perceptimi sa ka mashtrim mund të jetë po aq dëmtues për kredibilitetin e zgjedhjeve sa edhe vetë mashtrimi. Janë disa faktorë që kontribuojnë për këtë besim, duke përfshirë edhe perceptimin

[15] Një QR kod është një lloj barkodi tre-dimenzional, pjesën më të madhe të kohës përdoret për të koduar informacionin (URL apo detajet e kontaktit) dhe është dekoduar me ndihmën e aplikacionit të dedikuar në telefonin mobil; https://en.wikipedia.org/wiki/QR_code

[16] Mark Lindeman dhe Philip B. Stark, *Një prezantim i duhur për Rishikimin e Rreziqeve të Kufizimit*, *2012*; https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

[17] Qendra Belfer, *Libri për sigurinë kibernetike në zgjedhjet shtetërore dhe lokale, 2016*; https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

[18]Qendra Brennan, *Pajisjet e votimit në Amerikë në rrezik, 2015*; https://www.brennancenter.org/sitesdefault/files/publications/Americas_Voting_Machines_At_Risk.pdf

publik të vetë OMZ, ambientin politik, historia e mashtrimeve dhe keqpërdorimeve në një shtet specifik dhe sistem në vetë sistemin dhe mjetet e përdorura në procesin e zgjedhjeve. OMZ duhet të jetë vigjilente (e kujdesshme) në mbajtjen e një procesi transparent që lejon të gjithë palët e përfshira të besojnë se dhënia e votës, procesi i numërimit dhe vetë rezultatet janë legjitime.

Prezantimi i çdo teknologjie të re në një proces zgjedhor duhet të planifikohet me kujdes. [19] Një përvojë e parë negative ose një trajtim i dobët i një rrezikshmërie të ekspozuar – mund të kthejë palët e përfshira në zgjedhje kundër teknologjisë, dhe atëherë bëhet e vështirë për të rifituar besimin. Kjo ka ndodhura në disa shembuj: Referendumi i Barcelonës në Spanjë[20]kishte polemika në shumë mënyra, duke përfshirë vetë procesin e votimit, me raste të prezantimit të rrejshëm të raportuara dhe të dërguara në gjykatë; dhe shqetësimet e sigurisë të shprehur të publikut në Norvegji[21]dhe në Francë.[22] Përtej votuesve, drejtuesit e zgjedhjeve dhe stafi I tyre duhet gjithashtu t'i besojnë dhe të kuptojnë teknologjinë që ata përdorin në punën e tyre. Kjo mund të arrihet vetëm përmes proceseve rigoroze të vlerësimit dhe strategjive të trajnimit efektiv. Ofruesit e shërbimeve të jashtme duhet të jenë në pajtueshmëri me ligjet dhe kërkesat; nëse ofruesit e shërbimeve duket se janë në kundërshtim me ligjin, besimi i palëve të përfshira bie me shpejtësi. OMZ duhet të ndërmarrin një vlerësim një veçantë të rrezikut në lidhje me shoqëritë dhe të varurit të mundshëm të ofruesve të jashtëm të shërbimeve sepse këto lidhje mund të minojë kredibilitetin e sistemit të ri. Kjo nuk është e kufizuar me shitësit e sektorit privat, por gjithashtu të varurit e institucioneve tjera shtetërore.

Mësime nga Zvicra

Kantonet në Zvicër kanë ekperitmentuar me votimin përmes internetit, por numri i votuesve me të drejtë vote dhe që kanë marrë pjesë ka mbetur margjinal për shkak të testimeve dhe rishikimeve vijuese, kostot dhe besimit publik. Janë provuar paralelisht dy sisteme. Sistemi sVotë nga posta e Zvicrës është një sistem në pronësi, i shpalosur dhe zhvilluar ngaScytl. Ai ofron opsionin për ata votuesit me vendqëndrim në Zvicër dhe ata që janë jashtë shtetit të votojnë përmes aplikacionit mobil dhe faqes të internetit. Metoda e vërtetimit të votuesit është thelbësisht ndryshe nga ajo e Estonisë. Nuk mbështetet në një kartë të sofistikuar të ID, por në një kod të veçantë të sigurisë që u dërgohet atyre me postë; kërkohet regjistrim paraprak nga votuesit me qëllim që të marrin kodet e sigurimit. Pastaj votuesit duhet të shkruajnë numrat e tyre të votimit, kodet e veçanta të sigurisë, datën e lindjes dhe komunën nga e cila e kanë prejardhjen. Votimi zviceran përmes internetit ju nënshtrua një debati të nxehtë kur autoritetet organizuan një "shpërblim për gabimet", gjatë të cilit janë identifikuar dhe janë shpalosur rrezishmëritë respektivisht dobësitë kritike. Ky sistem tani është braktisur nga autoritetet zvicerane. Një sistem i dytë – Sistemi i Gjenevës – është ndërprerë gjithashtu së fundi. Rrjedhimisht, e ardhmja përmes internetit në Zvicër është e paqartë.

Përtej mundësive për mashtrim që janë të ekzaminuara më tutje në pjesën më poshtë për "Shqetësimet e sigurisë" administratorët e trajnuar dobët mund të krijojnë pa dashje gabime që bëjnë gërryerjen e

[19] Projekti ACEProject,*Parimet udhëheqëse për teknologjinë e zgjedhjeve– besimi dhe transparenca*;http://aceproject.org/main/engl ish/et/et20.htm

[20] *Lista e të dhënave në lidhje me referendumin e Barcelonës*, fq. 124; https://www.regjeringen.no/globalassets/upload/krd/prosjekter/e-valg/evaluering/topic6_assessment.pdf

[21] https://www.bbc.com/news/technology-28055678

[22] https://www.reuters.com/article/us-france-election-cyber/france-drops-electronic-voting-for-citizens-abroad-over-cybersecurity-fears-idUSKBN16D233

shpejtë të besimit publik. Votuesit të cilët nuk e kuptojnë se si të përdorin sistemin si duhet mund të bëjnë vetë gabimet, dhe më vonë ta atribuojnë këtë në keqpërdorimin e qëllimshëm nga ana e OMZ. Pilotimi dhe prezantimi i votimit përmes internetit duhet të bëhet të bëhet vetëm në kotekstin politik dhe social ku niveli i lartë i besimit në sistemin zgjedhor tashmë ekziston. Votimi përmes internetit si i tillë jo domosdoshmërisht do të rrisë besimin dhe në fakt mund ta zvogëlojë,[23]apo të shfrytëzohet si një mjet partiak apo politik. Ngjajshëm, mungesa e besimit të qytetarëve në paanshmërinë e stafit zgjedhor nuk do të rifitohet nga prezantimi i më shumë teknologjisë në proces; por në fakt ky besim ndërtohet nga lufta aktive kundër praktikave korruptive dhe rritjes të transparences. Keto çështje të besimit duhet të trajtohen në mënyrë gjithëpërfshirëse para se teknologjia të prezantohet në procesin zgjedhor.

Shqetësimet e sigurisë

Gjatë dekadës të kaluar, ka patur disa raste të profilit të lartë të sulmit mbi portalet e internetit, viruse që kanë mbyllur faqet e internetit të agjencive qeveritare dhe koorporatave të mëdha dhe softuerëve me qëllim të keq që ka gjymtuar organizatat duke koduar të dhënat e tyre. Duke patur parasysh se sa po rrezikohet për zgjedhje, mund të supozohet me arsye se aktorët me qëllime të këqija – sidomos në shtetet me kundështarë specifik gjeopolitik – mund të krijojnë dhe të shpërndajnë në mënyrë specifike programe me qëllime të këqija të dizajnuara për të manipuluar votën.

Nëse një virus nuk zbulohet nga një program antivirusi në kopmpjuterin e votuesit, mund të manipulojë votën e viktimës në favor të partisë specifike të sulmuesit. Gjithashtu ka mundësi për sulmuesit që të krijojnë një person si votues të rrejshëm, që mund të mashtrojë përdoruesit të mendojnë që ata kanë votuar, edhepse ata në fakt asnjëherë nuk janë qasur në sistemin zyrtarë apo nuk kanë dhënë votën. Nëse ndonjë prej këtyre sulmeve ndodh në shkallë të madhe, ata mund të minojnë vlefshmërinë e zgjedhjeve apo të gjithë sistemin zgjedhor.

Aktivitetet e mundshme me qëllime të këqija mund të përfshijnë parandalimin e votuesit që të jap votën e tij apo të saj, të ndryshojnë zgjidhjen e votuesit, të monitorojnë se si voton një voton, të përdorin kredencialet e votuesit për të fituar qasje dhe të zgjerojnë atë qasje për të dëmtuar sistemin e votimit, duke ndryshuar rezultatet e votimit apo dëmtojnë kredibilitetin e rezultateve zgjedhore. Vjedhja e kredencialeve, praktika e dërgimit të porosive elektronike mashtruese dhe inxhineringu social janë mënyra tjera të mundshme të sulmuarit të sistemeve zgjedhore, edhepse ata mund të mos ndikojnë një numër të madh të votuesve.

Zyrtarët zgjedhorë zakonisht kanë leje të nivelit më të lartë për të shtuar votuesit me të drejtë vote në bazën e të dhënave të listës zgjedhore, të hiqen votuesit që nuk kanë të drejtë vote, për të konfiguruar stilet e fletëve të votimit, për të përkufizuar kohën dhe datën për të dhënë votën, për të vendosur rregullat e përpilimit për kontestet zgjedhore, dhe për të gjeneruar raporte zgjedhore. Këta palë të interesit mund të kompromentojnë me qëllim të keq sistemin apo pa dashje të marrin pjesë në sulm përmes një pajisjeje të infektuar. Automatizimi dhe dhe kompjuterizimi i detyrave të zyrtarëve të shoqërohet me disa protokolle që do të parandalojnë sulmet e fshehta kundër sistemit, nivelet e

[23] Prezantimi i shpërblimit për gabim në Zvicër; https://www.theverge.com/2019/2/12/18221570/swiss-e- electronic-voting-public-intrusion-test-hacking-white-hack-bug-bounties

duhura të profileve të lajmërimit, fjalëkalimet dhe rishikimi, dhe trajnimet dhe programet e vetëdijes mbi rreziqet e sigurisë kibernetike.

Administratorët e sistemit kanë nivelin më të lartë në administrimin e serverit dhe sistemet tjera zgjedhore të informacioneve. Shumicën e kohës ata kanë qasje fizike në pajisje dhe u lejohet që të instalojnë, konfigurojnë dhe monitorojnë komponentat e ndryshme të sistemit të votimit për të siguruar që funksionon siç duhet. Ata mundet që pa dashje apo aksidentalisht të kontribuojnë në një sulm duke përdorur flash disqe USB të infektuara, për shembull, apo kur me dashje apo pa dashje e zvogëlojnë mbrojtjen e sistemit. Në mjedise të caktuara, kërcënimet personale kundër informacioneve kryesore dhe stafit të teknologjisë të komunikacionit duhet të merret parasysh, sepse ata mund të ofrojnë informacione që mund të shfrytëzohen nga kundërshtarët.

Mësime nga Uashington, D.C.

Në vitin 2010, Këshilli Zgjedhor i Qarkut të Kolumbisë ka lëshuar një ftesë të hapur për hakerët për të gjetur rrezikshmëritë në pilot programin e votimit përmes internetit për të lejuar votuesit jashtë shtetit dhe personelin ushtarak për të votuar në formë elektronike. Një ekip i udhëhequr nga hulumtuesit nga Universiteti i Miçiganit pati mundësinë që të ndërhyjë në sistem në më pak se 36 orë dhe ka fituar qasje në të gjithë identifikimet dhe lejekalimet e votuesve me të drejtë vote. Ata kanë modifikuar të gjithë votat në një kandidatë imagjinar pa u vërejtuar fare nga administratorët e programit, madje duke fituar qasje në sistemin e mbikqyrjes video të komisionit zgjedhor. Përmes artikujve të ndryshëm dhe intervistave elektronike, ky rast ka gjeneruar një diskutim të gjërë publik dhe është bërë një shembull se sa dëm mund të bëhet në kredibilitetit e komisionit zgjedhor kur ekspozohet një informacion i pasigurtë i sistemit. Në SHBA, votimi përmes internetit është përdorur në më shumë se 30 shtete,kryesisht për votuesit jashtë shtetit dhe për personelin ushtarak, pavarësisht paralajmërimeve dhe rekomandimeve nga ekspertët dhe komisionet e ndryshme.

Korniza e krimit kibernetik të Institutit Nacional të Standardeve dhe Teknologjisë (INST)[24]ofron disa rekomandime për të zbutur rreziqet kundër këtyre aktorëve. Kjo duhet të merret me kujdes – ata nuk lirojnë një organizatë për të performuar një modelim të tërësishëm të kërcënimit dhe plani menaxhimit të rrezikut, sepse asnjë strategji për sigurinë kibernetik nuk është tërësisht efektive. Në mes të rekomandimeve të tij, INST këshillon përdorimin e mbrojtjeve kriptografike (për transferimin e të dhënave dhe të dhënave jo aktive), të avancohen tekniket kriptografike të votiimit, përdorimi i harduerit të dedikuar dhe të besur (siç janë kartat e ID) skanimi i sigurisë të rrjeteve kompjuterike të lidhura në distancë me pajisjen e klentit (për të kontrolluar që një pjesë e softuerit që është përdorur për votim nuk është ndryshuar), mjedisi i konfigurimi para se të fillojë të punojë kompjuteri apo teknologjia virtuale (e vështirë për ta realizuar në pajisjet e të gjitë votuesve, por që mund të pengojë sistemet me qëllime të këqija) dhe kanalet e komunikimit dytësor (siç është kodi QR në Estoni për të kontrolluar votën e tyre me një pajisje alternative).

[24] Instituti Nacional i Standardeve dhe Teknologjisë në kërkesë të Komisionit Ndihmës Zgjedhorë të SHBA-së, *Konsideratat e Sigurisë për Votimin elektronik në distancë UOCAVA, 2011;* https://www.nist.gov/sites/default/files/documents/itl/vote/NISTIR-7700-feb2011.pdf

Votimi Elektronik Blockchain

Në tre vitet e fundit, ka patur një përpjekje të rritur për tregun e votimit elektronik. Me këtë rritje, kompanitë kanë filluar që të promovojnë përdorimin e blockchain si një "platformë" nga i cili fletëvotimet
mund të transmetohen nga pajisjet private të votuesve në objektin e centralizuar të përmbledhjes, duke pretenduar se siguron pronat e Sistemit për kontrollim të votimit elektronik.

Blockchain është një llojë e bazë e shpërndarë e të dhënave. Zakonisht është në pronësi dhe përdoret nga disa entitete të pavarura që veprojnë si kolegë. Çdo koleg regjistron transaksione të reja të cilat janë do koduara në formë kriptografike me nënshkrim të transaksioneve të mëparshme. Sipad dizajnit, një blockchain është rezistent ndaj modifikimit të të dhënave nga një koleg, një prone që quhet pandryshueshmëri. Në zgjedhje të bazuara në blockchain, blochkchain shërben si një kuti votimi e shpërndarë që mban fletëvotimet e hedhura, edhepse ndonjëherë përdoret për të mbajtur edhe informacione tjera. Një pikë themelore për blockchain është se mbështetet në faktin se ka shumë kolegë. Me vetëm një përdorues (koleg) – OMZ – nuk ka pandryshueshmëri të të dhënave dhe përfitimi i përdorimit të blockchain është humbur.
Për fat të keq, rrezikshmëritë më serioze që kërcënojnë integritetin dhe fshehtësinë e e votimit ndodhin para se fletëvotimet të arijnë blockchain.[25]Shumë nga këto zgjidhje nuk e zgjidhin çështjen e ID të votuesit, për shembull. Kjo është thelbësore për kredibilitetin e zgjedhjeve. Estonia, për shembull ka zgjidhur këtë çështje pa përdorur ID kartelat. Për më tepër, siguria e pajisjes përmes të cilës votuesit e japin fletëvotimin elektronik është në masë të madhe jashtë fushëveprimit të këtyre sistemeve të blockchain. Teknologjia blockchain gjithashtu nuk mbron nga sulmet e shpërndara të mohimit të shërbimit që i pamundësojnë serverët që të funksionojnë, nuk mbron informacionin përderisa qarkullon në internet dhe nuk e bën serverin dhe infrastrukturën më rezistente ndaj kërcenimeve të avancuara të vazhdueshme.

Mësime nga Gjermania

Gjykata Kushtetuese e Gjermanisë konsideron se çfarëdo votimi elektronik është jokushtetues për disa arsye: Votuesit duhet të vendosin besim të verbër në teknolologji dhe nuk kanë mënyrë për të ditur se si kompjuterët numërojnë fletëvotimet, dhe çdo sistem elektronik apo i ri duhet të jetë i kuptueshëm dhe i përdorshëm për personin laik se sistemi që ai po zëvendëson (laps dhe letër për një fletëvotim fizik që mund të preket). Kjo në thelb e bën çdo sistem të votimit elektronik të pamundshëm për ta zbatuar në Gjermani me nivelet aktuale të teknologjisë.

[25] David Jefferson (Votimi i kontrolluar), *Miti i Votimit Blockchain të "sigurtë"*; https://www.verifiedvoting.org/wp-content/uploads/2018/10/The-Myth-of-_Secure_-Blockchain-Voting-1002.pdf

Përfundim

Prezantimi i teknologjisë të re, siç është votimi përmes internetit, duhet që të përgjigjet në problemin specik. Para se të konsiderohet votimi në distancë përmes internetit, apo çfarëdo zgjidhje teknologjike, është kritike që OMZ identifikojnë çështjet në procesin zgjedhor që mundohet ta zbusë apo trajtojë. Nëse votimi në distancë përmes internetit besohet se trajton këtë problem, duhet atëherë të konsiderohet me kujdes para se të zbatohet. Përderisa teknologjia e re sigurisht që paraqet mundësi, mungesa e përgatitjes për shkak të kujdesit të duhur mund të shkaktojë një dëm të madh në besimin publik dhe integritetin e vetë zgjedhjeve. Ka mënyra të ndryshme të integrimit të teknologjisë të votimit në distancë, nga synimi i popullsisë kufizuese votuese për të cilat votimi është sfidë, deri në përpjekjen ambicioze për të përmirësuar daljen nacionale në votime dhe të zvogëlojë koston e votimit. Votimi në distancë përmes internetit; ekzistojnë rrugë të tjera për zgjidhjet elektronike. Ata që konsiderojnë votimin përmes internetit si një zgjidhje globale duhet të vlerësojmë me kujdes ndikimet e mundshme mbi koston, pjesëmarrjen, efikasitetin, besimin dhe sigurinë.

Ky dokument paraqet një pasqyrë të konsideratave kryesore nga literatura ekzistuese dhe nënvizon rastet e ndryshme. Kjo pasqyrë është paraparë që të inkurajojë studimin e mëtutjeshëm të kësaj teme para se të merren vendimet dhe të paraqesë një varg të gjërë të çështjeve dhe perspektiva për konsiderata. Këto përvoja gjithashtu sjellin me vete një masë të kujdesit:

- Konteksti politik dhe social ndryshon nga një shtet në tjetrin. Një përvojë e suksesshme në Estoni nuk do të thotë që ky model është i mirë për çdo shtet tjetër. Një pilotim i dështuar në një shtet mund të drejtojë palët e tij të interesit larg nga teknologjia për një afat të gjatë.
- Kostoja është një faktor i rëndësishëm. Të gjithë kostot duhet të llogariten siç duhet në filim të diskutimit për të siguruar që palët e interesit i kuptojnë kriteret në të cilat i bazojnë vendimet e tyre.
- Nuk ka një shembull të vetëm deri sot në të cilin votimi përmes internetit ka rritur pjesëmarrjen të votuesve.
- Korniza ligjore do të kërkojë përshtatjet e duhura për të lejuar përdorimin e teknologjisë të re gjatë votimit. Kjo mund të ndikojë në kohën e nevojshme për vendosur në tërësi teknologjinë në zgjedhje ligjërisht të detyrueshme.
- Prezantimi i teknologjisë nuk e rrit automatikisht besimin. Besimi mund të fitohet vetëm nga vendosja e duhur e procedurave dhe rishikimit dhe u ofron palëve të interesit me transparencë dhe qasje të mjaftueshme dhe informacion për të kuptuar në të tërësi sekuencën dhe mekanizmat e procesit të votimit. Besimi është ndërtuar që nga fillimi – OMZ duhet të kuptojë pilotimin dhe fazat e dizajnit duke përfshirë konsultimin me palët e jashtme të interesit.

- Votimi në distancë mund të ndikojë në fshehtësinë e votës. Pa mbikqyrjen e personave të procesit zgjedhor nga të punësuarit në vendvotim, për shembull, OMZ duhet të jetë i vetëdijshëm për mundësitë për presionin e jashtëm, blerjen e votës apo keqpërdorimin dhe të ndërmarrë masa për të bashkëvepruar me këtë.
- Siguria dhe ajo që është edhe më e rëndësishme, perceptimi i sigurisë, është një faktor kryesor që duhet të drejtojë bisedën reth votimit përmes internetit

Përderisa ka përfitime që shtetet mund të fitojnë nga pilotimi i votimit përmes internetit, sidomos për grupet specifike të votuesve siç janë personat me aftësi të kufizuara, personat e shpërngulur brenda shtetit, votuesit në territoret e okupuara apo në diaporë, rreziqet duhet të vlerësohen me kujdes. Shumë shtete janë larguar nga votimi përmes internetit- dhe votimi elektronik më gjërësisht- për shak të çështjeve të sigurisë dhe çështjet e sigurisë publike.

Shpërndarja e suksesshme e kësaj teknologjie ka treguar se duhet të ndërtohet me një infrastrukturë ekzistuese të fuqishme me të cilën qytetarët njihen dhe mbështeten për shërbime tjera, siç është Estonia, në vend se një platformë e re krijuar në mënyrë specifike për votimin përmes internetit.

Secila dhe të gjithë përpjekjet për të digjitalizuar procesin zgjedhor të shtetit – duke përfshirë votimin përmes internetit – duhet të konsiderohet me kujdes përmes studimit të fizibilitetit që inkorporon hulumtimin ndërkombëtar dhe kontekstin nacional. Kjo është në pajtim me praktikat e mira europiane dhe duhet t'i paraprijë pilotimit potencial dhe pjesëmarrjes pasuese.

Aneksi 1 – Resurset shtesë dhe dokumentacioni

Resurset themelore

1. Sigurimi i votës, mbrojtja e demokracisë amerikanë nga Akademia kombëtare e shkencave, inxhinierisë, dhe mjekësisë, 2018: https://www.carnegie.org/media/filer_public/34/9d/349d3207-d994-4838-8b79-5f8d88e0e412/nas_report.pdf
2. Ese nga Bruce Scheneier mbi Sigurinë e Votimit, 2004: https://www.schneier.com/essays/archives/2004/07/voting_security.html
3. Udhëzyes për *Zbatimin dhe Mbikqyrjen e Teknologjive të Votimit dhe Numërimit Elektronik* nga Fondacioni Ndërkombëtar për Sistemet Zgjedhore dhe Instituti Nacional Demokratik, 2003: https://www.ndi.org/sites/default/files/Implementing_and_Overseeing_Electronic_Voting_and_Counting_Technologies.pdf

Resurset dhe Dokumentacionet tjera të rëndësishme

1. Votimi elektronik: Shpërblimet dhe rreziqet, Raport nga Këshilli Atlantik dhe McAfee, 2014: https://www.verifiedvoting.org/wp-content/uploads/2014/10/Online_Voting_Rewards_and_Risks.pdf
2. "Votimi elektronik: e kaluara, e tashmja dhe e ardhmja" Fondacioni Ndërkombëtar për Sistemet Zgjedhore, Ben Goldsmith, 2013: https://www.ifes.org/news/Internet-voting-past-present-and-future
3. Dokument i shkurtër i Parlamentit Europian, *Teknologjia Digjitale në Zgjedhje: Efikasiteti kundrejt Kredibilitetit,* ,2018, https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI(2018)625178_EN.pdf
4. *Prezantimi i Votimit Elektronik: Konsideratat themelore, IDEA Ndërkombëtare* , 2011: https://www.idea.int/sites/default/files/publications/introducing-electronic-voting.pdf
5. *Emaili dhe Votimi përmes internetit: Kërcënimi i pavërejtur në Sigurinë e Zgjedhjeve*, Susan Greenhalgh– Koalicioni Nacional i Mbrojtjes Zgjedhore, Susannah Goodman – Fondi i Përbashkët për Kauzën e Edukimit, Paul Rosenzweig, R Street Institute, Jeremy Epstein, ACM Komiteti i SHBA-së për Politika Teknologjike, 2016: https://www.acm.org/binaries/content/assets/public-policy/jtreportemailInternetvoting.pdf
6. *Studimi i Fizibilitetit mbi Votimin përmes Internetit për Komisionin Qëndror Zgjedhor të Republikës të Moldavisë*, 2016: https://www.undp.org/content/dam/moldova/docs/Publications/MD-IVOTE-FS- and-Roadmap_cleanENG.pdf
7. Hakimi i D.C Pilotimi i votimit përmes internetit, 2010 nga J. Alex Halderman, https://jhalderm.com/pub/papers/dcvoting-fc12.pdf, https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offer- online-voting-but-experts-warn-it-isnt-secure/, https://www.youtube.com/watch?v=tHJlRkwOd4U dhe https://www.youtube.com/watch?v=G4myYkbtkuk
8. Raporti i misionit për vlerësimin e nevojave nga Organizata për Siguri dhe Bashkëpunim në Europë për Zgjedhjet e Nëntorit të vitit 2019 të Asamblesë Federale, duke siguruar një analizë mbi çështjet e identifikuara dhe rekomandime të mëtutjeshme dhe konteksti mbi votimin përmes internetit.

, https://www.osce.org/odihr/elections/switzerland/425009?download=true

9. Vlerësimi i programit të pilotimit të e-votimit nga Ministria e Pushtetit Lokal të Norvegjisë: https://www.regjeringen.no/en/historical-archive/Stoltenbergs-2nd-Government/Ministry-of- Local-Government-and-Regiona/tema-og-redaksjonelt-innhold/kampanjesider/e-vote- trial/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trials-in-201/summary-of-the- isf-report/id685824/
10. Fondacioni Ndërkombëtar për Sistemet Zgjedhore, "Përvoja Ndërkombëtare me E-votimin, Projekti norvegjez E-Vote"ngaJordi Barrat Esteve,Ben GoldsmithdheJohnTurner,2012: https://www.regjeringen.no/en/historical-archive/Stoltenbergs-2nd-Government/Ministry-of- Local-Government-and-Regiona/tema-og-redaksjonelt-innhold/kampanjesider/e-vote- trial/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trials-in-201/id684642/

Aneksi 2 – Shtetet që përdorin votimin përmes internetit (Përdorimi i votimit përmes internetit jashtë vendvotimeve Zgjedhje të detyrueshme politike)

E përdorur në të gjithë shtetin	E përdorur në disa pjesë të shtetit apo disa llojë të votuesve	Planifikohet të pilotohet, ose është pilotuar por është ndërprerë ose nuk është përdorur asnjëherë
Estonia është shteti i vetëm që lejon të gjithë qytetarëve opsionin të votimit elektronik në zgjedhjet lokale, nacionale dhe europiane.	**Armenia**: Stafi diplomatik dhe familjet e tyre mund të votojnë në formë elektronike.	**Francë**: Votimi është përdorur për votuesit jashtë shtetit në zgjedhjet parlamentare të vitit 2012 por është ndërprerë në vitin 2017 për shqetësime sigurie; qeveria planifikon ta rikthejë në vitin 2022. Banorët jashtë vendit gjithashtu votuan në formë elektronike në zgjedhjet parësore Republikane në vitin 2016.
	Australia: Votimi elektronik ishte në provë për personelin ushtarak jashtë vendit në vitin 2017 por është ndërprerë. Uellsi i Ri Jugor lejon disa grupa – personat me aftësi të kufizuara, që jetojnë në zona në distancë, jashtë shtetit – të votojnnë në formë elektronike por nuk ka një plan për ta zgjeruar këtë mundësi në shtetet tjera.	**India**: Në vitin 2010, votimi përmes internetit është provuar në zgjedhjet lokale në shtetin e Gujarat.
	Kanadë: Votimi elektronik është mundshëm për zgjedhjet komunale në disa qarqe të Ontarios dhe Nova Scotias. Kanada ka menduar prezantimin e votimit përmes internetit në zgjedhjet federale.	**Norvegjia:** Votimi elektronik për zgjedhjet lokale të vitit 2011 dhe parlamentare të vitit 2013 është bërë i disponueshëm në disa qarqe. Në vitin 2014, votimi përmes internetit është ndërprerë për arsye sigurie.
	Meksika: Disa shtete kanë lejuar votimin elektronik për votuesit jashtë shtetit.	Në vitin 2004, **Hollanda** ka përdorur votimin përmes internetit për zgjedhjet në këshillin ujor *Rijnland,* në vitin 2006 për votuesit jashtë shtetit për zgjedhjet nacionale. Votimi përmes internetit është ndërprerë në vitin 2017 për shqetësime sigurie.

	Zelanda e re: Votuesit jashtë shtetit mund të votojnë në formë elektronike.	**Spanja**: Në vitin 2010, Barcelona ka mbajtur një referendum në formë elektronike për një projekt të zhvillimit urban. Votimi ishte vetëm njëherë, pilotim vetëm në formë elektronike dhe kishte shumë polemika.[26]
	Panama: Votuesit jashtë shtetit mund të votojnë në formë elektronike	**Mbretëria e Bashkuar:** Votimi elektronik është provuar në zgjedhjet e këshillit lokal ndërmjet 2002 dhe 2007.
	Zvicra: Disa kantone ofrojnë votimin elektronik për votuesit jashtë shtetit – gjithashtu në disa raste, për votuesit me vendqëndrim - në zgjedhje dhe referendum. Synimi i shtetit është që të rrisë votimin në të gjithë shtetin.	**Rusia** është e vendosur për të prezantuar sistemin e parë të votimit elektronik. Sistemi do të testohet në një lagje në Moskë që do të zgjedhin një anëtarë të vetëm këshillin e kryqytetit në shtator të vitit 2019. Një nga eksperimentet e para për të prezantuar votimin përmes internetit ishte kryer nga Komisioni Zgjedhor në Rajonin e Volgogradit gjatë votimit në Uryupinsk në vitin 2009, dhe në qarkun e Odintsovo në vitin 2010.
	Shtetet e Bashkuara: Pavarësisht shqetësimeve të sigurisë të ngritura pas provës në Qarkun e Kolumbisë ku është hakuar votimi përmes internetit, më shumë se 30 shtete në SHBA lejojnë personelin ushtarak dhe banorët jashtë shteti të votojnë në formë elektronike. Votuesit që përdorin fletëvotimet elektronike apo me postë heqin dorë nga të drejtat e fshehtësisë.	**Finlanda** ka zgjedhur një grupë pune të studiojë fizibilitetin teknik e një sistemi të votimit elektronik. Ka përcaktuar se teknologjia nuk përmbush mjaftueshëm të gjithë kërkesat, duke theksuar problemet me pajtimin e kontrollimit dhe fshehtësinë zgjedhore.

Burimi: http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI(2018)625178_EN.pdf

[26] Qyteti spanjoll i Barcelonës ka hasur problem në lidhje me identifikimin e votuesit, dhe vjedhjen e identitetit me gjetje të spikatur të votuesve që dikush tashmë është lajmëruar me detajet e tij atë autentifikimit dhe ka votuar për të; https://www.regjeringen.no/globalassets/upload/krd/prosjekter/e-valg/evaluering/topic6_assessment.pdf

Për autorët

Meredith Applegate, Këshilltare Programi në IFES, Ukrainë

Meredith Applagate është këshilltare progami e IFES në Ukrainë. Ajo sjell mbi 10 vite përvojë në zhvillimin, menaxhimin dhe realizimin e programeve zgjedhore dhe demokratike në seli dhe në terren. Ajo është në veçanti e fokusuar në barazinë gjinore, avokimin dhe zhvillimin e shoqërisë civile, edukimin e votuesve dhe qytetarëve, dhe të drejtat e personave me aftësi të kufizuara.
Applegateka mbajtur për një kohë të gjatë pozita në Indonezi, Mianmar dhe Ukrainë. Ajo gjithashtu ka punuar në detyra afatshkurte dhe afatmesme mbi operacionet zgjedhore, edukimin e qytetarëve dhe votuesve, dhe përfundimin e dhunës kundër grave në zgjedhje, duke përfshirë për Entitetin e Kombeve të Bashkuara për Barazi Gjinore dhe Fuqizimin e Grave në Sierra Leone, Programi për Zhvillim i Kombeve të Bashkuara në Moldavi, dhe programet e IFES në Kamboxha, Republikën Domenikane, Nepal dhe Timor-Leste.

Vladlen Basysty, Menaxher i Teknologjisë dhe Sigurisë Kibernetike në IFES, Ukrainë

Vladlen Basysty është menaxheri i teknologjisë dhe sigurisë kibernetike për IFES në Ukrainë. Basysty ka 16 vite përvojë në menaxhimin e projekteve të teknologjisë të informacionit me organizatat duke përfshirë Organizatën Ndërkombëtare për Migracion, CGI Federal, Ambasadën e Shteteve të Bashkuara në Ukrainë, Zyra e Departamentit të Shteteve të Bashkuara për Sigurinë e Atdheut, Qendra Federale për trajnimin e zbatimit të ligjir, Instituti John Snow / projekti i Agjencisë së Shteteve të Bashkuara për Zhvillim Ndërkombëtar, "AIDS Fondacioni Lindje-Perëndim," dhe Vullnetarët e Paqes të Shteteve të Bashkuara në Ukrainë.

Thomas Chanussot, Ekspert i lartë për Teknologjinë e Zgjedhjeve dhe Sigurinë Kibernetike

ThomasChanussot ka punuar në fushën e zgjedhjeve që në vitin 2004. Me profil profesional në teknologjinë e informacionit, ai është përfshirë në më shumë se 12 operacione zgjedhore reth botës, sidomos në listat zgjedhore dhe teknologjinë e menaxhimit të rezultateve, ku gjatë kësaj kohe ka mbajtur role të ndryshme duke përfshirë zhvillimin e sistemit, rishikimet e sigurisë dhe menaxhimi i ekipit. Ai ka punuar gjërësisht në infrastrukturën kritike të misionit zgjedhor, duke siguruar bazat e të dhënave biometrike dhe jobiometrike të listave zgjedhore, si dhe sistemet për menaxhimin rezultateve. Ai tani menaxhim disa iniciative kritike të sigurisë kibernetike të zgjedhjeve në Azi dhe Europën Juglindore dhe udhëheq vlerësimet e sigurisë kibernetike për IFES.

Ekspertizë Globale. Zgjidhje lokale
Demokraci të qëndrueshme

IFES | 2011 Crystal Drive | 10th Floor | Arlington, VA 22202 | www.IFES.org