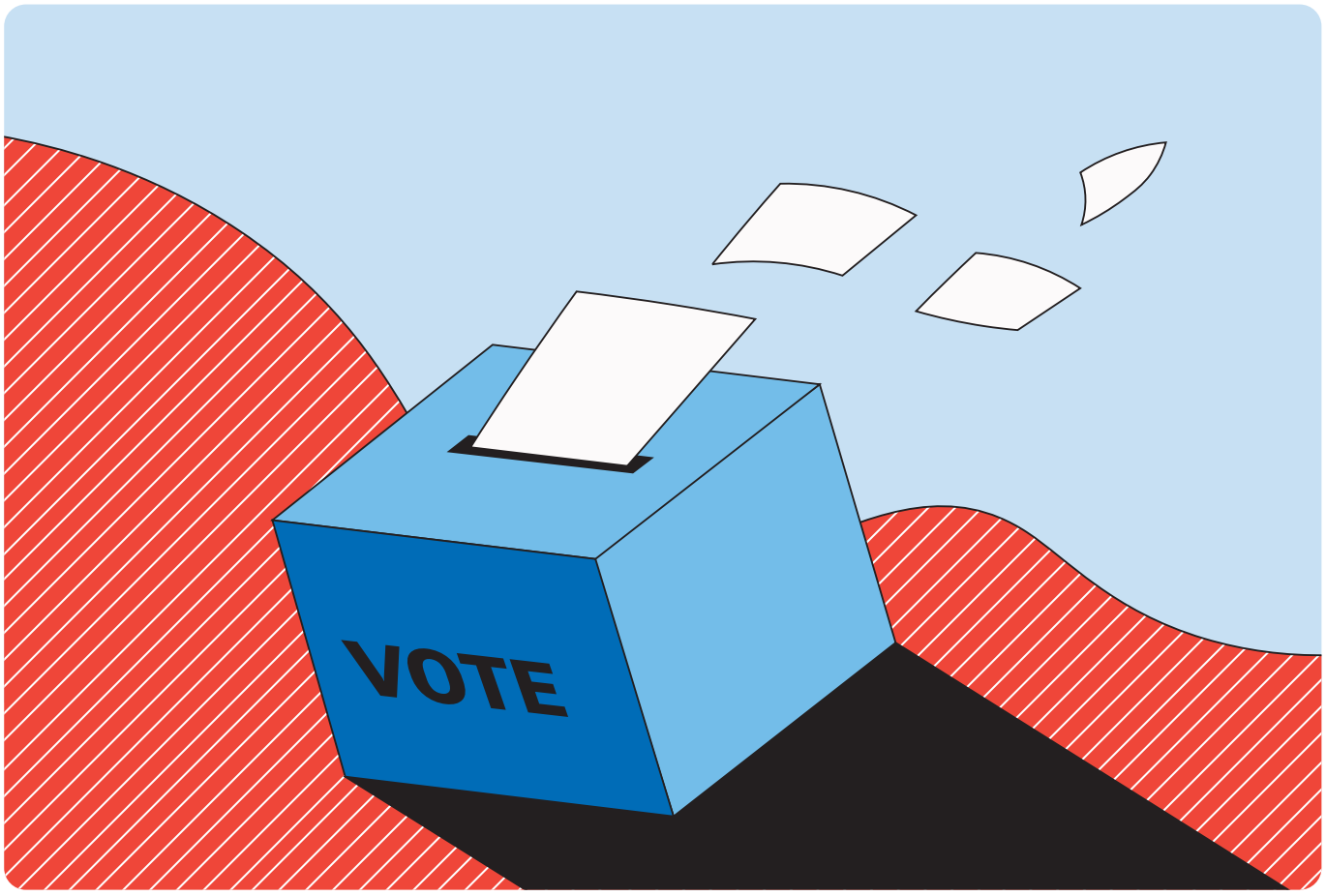
Ընտրությունների պաշտպանությունը հիբրիդային սպառնալիքներից.

Պաշտպանական գործնական ուղեցույց

Սեբաստիան Բեյ և Կատալինա Ուրիբե Բուրչեր
2025 թվականի նոյեմբեր



Ֆոլկե Բեռնադոտ ակադեմիա
Խաղաղության, անվտանգության և զարգացման շվեդական գործակալություն

FBA

Երախտիքի խոսք

Այս զեկույցի հեղինակները ցանկանում են իրենց երախտագիտությունը հայտնել բազմաթիվ անհատներին և թիմերին, որոնց ներդրումների շնորհիվ հնարավոր դարձավ դրա պատրաստումը:

Նախևառաջ, ցանկանում ենք շնորհակալություն հայտնել Լիզա Օրենիուսին, ով վերահսկել է գործընթացը սկզբից մինչև վերջ և տրամադրել է շարունակական արձագանք և ուղղորդում: Մեր շնորհակալությունն ենք նաև հայտնում Ֆոլկե Բերնադոտ ակադեմիայի (FBA) գործընկերներին, ովքեր վերանայել և մեկնաբանել են կառուցվածքը, բովանդակությունը և շրջանակը, այդ թվում՝ Ժողովրդավարության և կառավարման բաժնից Կարլ Ֆրեդրիկ Բիրկոֆին, Ֆիլիպա Ալմլունդին և Կիկի Վեստինին, ինչպես նաև հետազոտական թիմից Էմմա Սկեպստրյոմին և Աբդալհադի Ալիջլային:

Մեր երախտագիտությունն ենք հայտնում Սուսաննա Կույանպյային՝ (նախկինում՝ Հիբրիդային սպառնալիքների դեմ պայքարի եվրոպական գերազանցության կենտրոնի, Հիբրիդային ԵԽ) իր արժեքավոր արտաքին վերլուծության և խորաթափանց մեկնաբանությունների համար:

Հատուկ շնորհակալություն Այնա Բորիսին, ով վերահսկել է բոլոր արտադրական մանրամասները և ապահովել, որ ձեռագիրը, էջերի դասավորությունը, նկարազարդումները և հանձնումը սահուն կերպով համադրվեն: Նաև շնորհակալություն ենք հայտնում Essen International-ին և Comactiva Language Partner-ին՝ տեքստերի խմբագրման, էջերի դասավորության և նկարազարդումների գործում իրենց գերազանց աշխատանքի համար:

Հրաժարում

Այս զեկույցում արտահայտված տեսակետները պատկանում են հեղինակներին և պարտադիր չէ, որ արտացոլեն Ֆոլկե Բերնադոտ ակադեմիայի (FBA) կամ Շվեդիայի կառավարության պաշտոնական քաղաքականությունը կամ դիրքորոշումը: Բովանդակության համար պատասխանատվությունը կրում են բացառապես հեղինակները: Կոնկրետ հաստատությունների, ընկերությունների կամ ապրանքների հիշատակումը չի ենթադրում FBA-ի կողմից հավանություն:

Պարունակություն

Նախաբան

Ազատ ընտրությունները ժողովրդավարական կառավարման անկյունաքարն են: Դրանք մարմնավորում են քաղաքացիների և պետության միջև սոցիալական պայմանագիրը՝ առաջարկելով ինչպես կառավարման միջոցներ, այնպես էլ՝ հաշվետվողականության մեխանիզմ: Այսօր այդ պայմանագիրն ավելի ու ավելի է ենթարկվում հարձակման: Հիբրիդային սպառնալիքները, որոնք միավորում են տեղեկատվական մանիպուլյացիաները, կիբեռհարձակումները և քաղաքական գործընթացների ապօրինի ֆինանսավորումը, թիրախավորում են ոչ միայն ընտրական գործընթացները, այլև այն վստահությունն ու սոցիալական կառուցվածքը, որից կախված է ժողովրդավարությունը:

Այս սպառնալիքները ո՛չ դրվագային են, ո՛չ էլ երկրորդական: Դրանք ներկայացնում են ժողովրդավարական կառավարմանն ուղղված կայուն և շատ հարմարվող մարտահրավեր: Սպառնալիքների և հարձակումների նպատակը միայն կոնկրետ որոշակի քվեարկության արդյունքի վրա ազդեցություն գործելը չէ, այլև ինստիտուտների նկատմամբ վստահությունը քայքայելը, պառակտումը խորացնելը և հասարակությունները ներսից թուլացնելը: Արհեստական բանականության և այլ զարգացող տեխնոլոգիաների կիրառումն ավելի է արագացրել այս միտումը՝ նվազեցնելով միջամտության արգելքները և մեծացնելով դրա ազդեցությունը:

Ֆոլկե Բեռնադոտ ակադեմիայի (FBA) համար ժողովրդավարության պաշտպանությունը հակամարտությունների կանխարգելման հիմնասյուն է և ազգային ու միջազգային անվտանգության հարց: Այն պահանջում է ոչ միայն տեխնիկական երաշխիքներ. այլ քաղաքական տեսլական, ինստիտուցիոնալ դիմակայունություն և միասնական կամք: Արդյունավետ արձագանքները պետք է ամրապնդեն բոլոր մակարդակներում ազգային դերակատարների համատեղ գործելու կարողությունը՝ այն ընդհանուր ըմբռնման ներքո, որ ժողովրդավարական դիմակայունությունը կախված է հասարակության բոլոր շերտերի ներգրավվածությունից: Միևնույն ժամանակ, այս ջանքերը պետք է պահպանեն ժողովրդավարական համակարգերին բնորոշ բացությունը, թափանցիկությունը և իրավունքները: Հիբրիդային սպառնալիքների դեմ պայքարը չի կարող լինել այն արժեքների հաշվին, որոնք ձգտում ենք պաշտպանել:

Այս զեկույցն արտացոլում է FBA-ի հանձնառությունը՝ աջակցելու ազատ և օրինական ընտրությունների ջանքերին: Այն համախմբում է գործնական պատկերացումներ՝ ուսումնասիրելու համար, թե ինչպես են հիբրիդային սպառնալիքները դրսևորվում տեղեկատվական գործողությունների, ապօրինի ֆինանսավորման և կիբեռհարձակումների միջոցով, և թե ինչպես կարող են համակարգված, կառավարման վրա կենտրոնացած ռազմավարություններն ամրապնդել ընտրական գործընթացի անխաթարությունը: Զեկույցի առաջարկություններն ընդգծում են «ամբողջ կառավարության» և «ամբողջ հասարակության» ներգրավման մոտեցումների կարևորությունը, համագործակցության ցանցերի ինստիտուցիոնալացումը և ընտրությունների օրվանից հետո պատրաստվածության շարունակական շրջափուլը:

Իր էությամբ, զեկույցը պնդում է, որ ընտրական դիմակայունությունն անբաժանելի է ժողովրդավարական դիմակայունությունից: Հիբրիդային սպառնալիքների դեմ պաշտպանական կարողությունների ձևավորումը միայն անվտանգության վարժանք չէ. այն ներդրում է օրենքի գերակայության, հաշվետու կառավարման և ժողովրդավարական ինստիտուտների կայուն արժանահավատության մեջ:

Այս զեկույցում ներկայացված օրինակներն ու դասերը վերաբերում են բոլոր երկրներին, ներառյալ մեր սեփական երկրին՝ Շվեդիային: Հիբրիդային սպառնալիքները սահմաններ չեն ճանաչում, ինչպես նաև չեն տարբերակում հասուն և զարգացող ժողովրդավարությունները: Նույն մարտավարությունները, որոնք մի համատեքստում փորձում են խաթարել ընտրական գործընթացի անխաթարությունը, կարող են արագորեն տեղափոխվել մեկ այլ համատեքստ: Հետևաբար, դիմակայունության ամրապնդումը համատեղ պատասխանատվություն է՝ թե՛ պետությունների, թե՛ հաստատությունների և թե՛ հասարակությունների միջև: Սովորելով տարբեր փորձառություններից և խթանելով անդրսահմանային համագործակցությունը, մենք կարող ենք ամրապնդել ոչ միայն ընտրությունների պաշտպանությունը, այլև հենց ժողովրդավարության հիմքերը:

Փեր Օլսոն Ֆրիդ
Գլխավոր տնօրեն
Ֆոլկե Բեռնադոտ ակադեմիա

Տերմինների բառարան

- **Շարունակական թիրախային հարձակումներ (APT).** Մեծ ռեսուրսներով, նպատակաուղղված հարձակումների դերակատարներ՝ հաճախ պետության կողմից հովանավորվող կամ պետության կողմից առաջադրանք ստացած, որոնք իրականացնում են երկարատև, առավելագույնս աննկատ ներթափանցումներ, ռազմավարական նպատակներին (լրտեսություն, նախնական դիրքավորում, խափանում կամ ազդեցություն) աջակցելով՝ թիրախային ցանցեր մուտք գործելու և այդ մուտքը պահպանելու համար:

- **Համակարգված, ոչ վավերական վարքագիծ (CIB).** Խաբուսիկ կամ ոչ իսկական հաշիվների համակարգված օգտագործում՝ բովանդակության ծագման, ինքնության կամ հանրաճանաչության վերաբերյալ մարդկանց մոլորեցնելու համար:

- **Դիփֆեյք.** Արհեստական բանականության տեխնիկաներով ստեղծված սինթետիկ կամ մանիպուլացված մեդիա՝ (պատկեր, աուդիո կամ տեսանյութ) տեղի չունեցող իրադարձությունները կամ խոսքը պատկերելու համար:

- **Ապատեղեկատվություն.** Կեղծ կամ մոլորեցնող տեղեկատվություն, որը ստեղծվել և տարածվել է միտումնավոր՝ անձին, սոցիալական խմբին, կազմակերպությանը կամ երկրին վնաս հասցնելու համար:

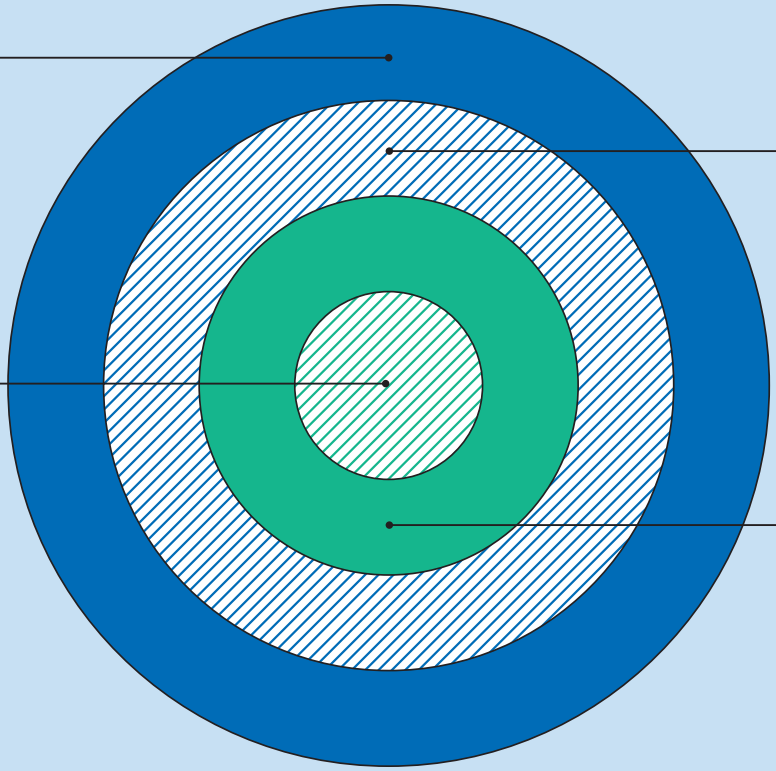
- **«Կրկնօրինակ» տեխնիկա.** Մարտավարություն, որն օգտագործում է «կրկնօրինակ» («doppelgänger») ենթակառուցվածք՝ կլոնավորված կամ մանրակրկիտ կեղծված լրատվական և ինստիտուցիոնալ կայքեր, դոմեյններ և սոցիալական հաշիվներ՝ սխալ կամ մոլորեցնող բովանդակությունը «լվանալու» համար՝ դրան թվացյալ վստահելի աղբյուրներից բխող տեսք տալով: Այնուհետև բովանդակությունը տարածվում և ուժեղացվում է համակարգված ոչ իսկական վարքագծի, վճարովի գովազդի և տարբեր հարթակներում վերահրապարակման միջոցով:

- **Դոքսինգ (երբեմն գրվում է «doxxing»).** Անձի մասին գաղտնի, անձնական կամ զգայուն տեղեկատվության առցանց հրապարակում կամ տարածում առանց նրա համաձայնության, սովորաբար՝ ոտնձգության, վախեցնելու կամ այլ կերպ վնաս պատճառելու նպատակով:

- **Օտարերկրյա տեղեկատվական մանիպուլյացիա և միջամտություն (FIMI).** Օտարերկրացի պետական կամ ոչ պետական դերակատարների (ներառյալ նրանց լիազորված անձանց) կողմից միտումնավոր և համակարգված կերպով իրականացվող մանիպուլյատիվ վարքագծի հիմնականում ոչ անօրինական ձև, որը սպառնում է արժեքներին, ընթացակարգերին և քաղաքական գործընթացներին կամ ունի դրանց վրա բացասաբար ազդելու ներուժ:

- **Հաքերային հարձակումների և արտահոսքի գործողություն.** Համակարգված գործողություն, որը նպատակ ունի վնաս հասցնել համակարգերին՝ տվյալներ գողանալու և ռազմավարական պահերին ընտրված, խմբագրված կամ

ՏԵՐՄԻՆԱԲԱՆՈՒԹՅԱՆ



Հիբրիդային սպառնալիքներ
Համակարգված, դիտավորյալ և վնասակար գործունեության լայն համատեքստը, որը ներառում է տեղեկատվություն, կիբեռ և ֆինանսական միջոցներ:

Ապատեղեկատվություն
Կեղծ կամ մոլորեցնող տեղեկատվություն, որը միտումնավոր տարածվում է վնաս պատճառելու նպատակով:

Տեղեկատվական ազդեցության գործողություններ (IIA)
Պլանավորված ջանքեր՝ տեղեկատվության և հաղորդակցության միջոցով ընկալումներ, վերաբերմունք կամ վարքագիծ ձևավորելու համար:

FIMI
Օտարերկրյա գործակալների կողմից իրականացվող մանիպուլյատիվ վարքագծի նմուշ՝ միտումնավոր և հաճախ համակարգված:

մանիպուլացված նյութեր հրապարակելու համար՝ լրատվական նարատիվների, հանրային ընկալման կամ քաղաքական գործընթացների վրա ազդելու համար:

- **Հիբրիդային սպառնալիքներ.** Համակարգված, միտումնավոր և վնասակար գործողություններ, որոնք միտումնավոր թիրախավորում են ժողովրդավարական պետությունների և ինստիտուտների համակարգային խոցելիությունները՝ ավանդական և ոչ ավանդական միջոցների համադրությամբ: Այս գործողությունները շահագործում են հայտնաբերման և պատասխանատու կողմի նույնականացման (վերագրելիության) սահմանափակ հնարավորությունները, ինչպես նաև պատերազմի ու խաղաղության, ներքին և արտաքին անվտանգության հատման գոտիները: Դրանք սովորաբար նպատակ ունեն ազդելու տեղական, պետական կամ ինստիտուցիոնալ մակարդակով որոշումների կայացման վրա՝ մնալով զինված հակամարտության շեմից ցածր:

- **Տեղեկատվական ազդեցության գործողություններ (IIA).** Պլանավորված ջանքեր՝ տեղեկատվության և հաղորդակցության միջոցով ընկալումներ, վերաբերմունք կամ վարքագիծ ձևավորելու համար: Այս գործողությունները ներառում են օրինական հանրային շփումից և դիվանագիտությունից մինչև գաղտնի կամ խաբուսիկ գործելակերպ, ինչպիսիք են անձնավորում/նմանակումը և համակարգված ոչ իսկական վարքագիծը: IIA-ն ընդհանուր տերմին է, որը ներառում է նաև FIMI-ն, որը վերաբերում է մասնավորապես օտարերկրյա պետական կամ ոչ պետական դերակատարների և նրանց լիազորված անձանց կողմից իրականացվող մանիպուլյատիվ վարքագծին:

- **Սխալ տեղեկատվություն.** Կեղծ տեղեկատվություն, որը, սակայն, չի ստեղծվել կամ տարածվել վնաս պատճառելու մտադրությամբ:

- **Նախահերքում.** Պրոակտիվ, պատվաստման (ինոկուլյացիայի) վրա հիմնված հաղորդակցման ռազմավարություն, որը նախազգուշացնում է մարդկանց հնարավոր մանիպուլյացիոն մեթոդների կամ նարատիվների մասին՝ նախքան դրանց հանդիպելը: Այն տրամադրում է պարզ, ճշգրիտ հաշվիչներ և որոշումների կայացման օժանդակ միջոցներ՝ օգնելու անհատներին ճանաչել և դիմադրել մանիպուլյացիային, երբ այն տեղի է ունենում: Ընտրական համատեքստերում նախահերքումը հաճախ իրականացվում է տեղեկատվության կենտրոնացված վստահելի հարթակի, հաճախ տրվող հարցերի և ժամանակին պլանավորված հանրային հաղորդագրությունների միջոցով՝ կապված հայտնի ռիսկային ժամանակահատվածների հետ (օր.՝ գրանցման վերջնաժամկետներ կամ քարոզչության լռության ժամանակահատվածներ):

- **Թիրախային ֆիշինգ.** Թիրախային հարձակում մարդկային գործոնի շահագործմամբ, որն օգտագործում է հատուկ խայծեր՝ կոնկրետ անձին խաբելու համար՝ գաղտնաբառերը բացահայտելու, մուտքի իրավունք ստանալու կամ վնասակար կոդ գործարկելու նպատակով:

- **Վիշինգ (կամ ձայնային ֆիշինգ).** մարդկանց մոլորեցման միջոցով իրականացվող խաբեություն հեռախոսազանգերով, որը հաճախ օգտագործում է զանգահարողի նույնականացման կեղծումը՝ անձանց ստիպելու բացահայտել տեղեկություններ կամ տրամադրել հասանելիություն:

Հապավումներ

- **AI.** Արհեստական բանականություն
- **APT.** Շարունակական թիրախային հարձակումներ
- **CaaS.** Կիբեռհանցագործությունը որպես ծառայություն
- **DDoS.** Բաշխված ծառայությունը մերժելու հարձակում
- **DSA.** ԵՄ թվային ծառայությունների մասին օրենք. մեծ առցանց հարթակների վրա դնում է վտանգների նվազեցման, թափանցիկության և տվյալների հասանելիության պարտավորություններ:
- **EMB.** Ընտրությունների կառավարման մարմին
- **FBA.** Ֆոլկե Բեռնադոտ ակադեմիա
- **FIMI.** Օտարերկրյա տեղեկատվական մանիպուլյացիա և միջամտություն

Ամփոփագիր

Սույն զեկույցը ներկայացնում է ընտրություններին սպառնացող հիբրիդային սպառնալիքների և դրանց արդյունավետ հակազդելու եղանակների համապարփակ վերլուծություն: Այն հիմնականում կենտրոնանում է 2024 թվականից ի վեր ընտրական միջամտության հիմնական ուղիներում տեղի ունեցած զարգացումների վրա, ներառյալ՝ օտարերկրյա տեղեկատվական մանիպուլյացիան և միջամտությունը (FIMI), քաղաքական գործընթացների ապօրինի ֆինանսավորումը և կիբեռգործողությունները: Չնայած առանձին վերլուծվում են, գործնականում դրանք սերտորեն փոխկապակցված են: Զեկույցն առաջ է քաշում գործնական պաշտպանական շրջանակ, որը զուգակցում է ինստիտուցիոնալ կարողությունների զարգացումը ցանցային, ամբողջ հասարակության աջակցության համակարգի հետ:

Հիմնական միտումները (2024 թվականից ի վեր).

- FIMI-ն վերածվել է կայուն արդյունաբերական մասշտաբի գործողությունների, որոնք ղեկավարվում են համակարգված ցանցերի, այլ ոչ թե մեկուսացված արշավների միջոցով:

- AI-ն և ավտոմատացումն արագացրել են սինթետիկ և խաբուսիկ բովանդակության ստեղծումն ու տարածումը, ինչպես նաև նվազեցրել են մարդկանց մոլորեցման վրա հիմնված խաբեության իրականացման ծախսերը:

- Քաղաքական գործընթացների ապօրինի ֆինանսավորումը, ներառյալ՝ միջնորդավորված ֆինանսավորումը, կրիպտոարժույթների միջոցով միջազգային փոխանցումները և անթափանց առցանց ծախսերը, ավելի ու ավելի են նպաստում մանիպուլյացիաներին և ընտրակաշառքին:

- Կիբեռգործողությունները խաթարում են ընտրական ենթակառուցվածքները և հաճախ գործում են տեղեկատվական գործողությունների հետ զուգահեռ՝ ուժեղացնելով դրանց ընդհանուր ազդեցությունը:

Այս միտումների հիմնական հետևանքն այն է, որ հակառակորդներն օգտվում են ընտրությունների կազմակերպման և աջակցման համար պատասխանատու հաստատությունների միջև եղած բացերից: Մեկուսացված արձագանքները հանգեցնում են անբավարար արդյունավետության: Սույն զեկույցը համախմբում է հակազդեցության լավագույն փորձը և ընդգծում այն գաղափարը, որ ընտրությունները այս բարդ սպառնալիքներից պաշտպանելու համար անհրաժեշտ է.

- Հստակ պատասխանատվություն, ռեսուրսներ, մանդատներ, անձնակազմ և յուրաքանչյուր գործակալության ներսում նախապես մշակված ու փորձարկված գործելակարգեր:

- Տարվա ընթացքում մշտապես գործող ազգային համագործակցության ցանց՝ հետախուզական տվյալներ փոխանակելու, համատեղ վարժանքներ անցկացնելու և պաշտպանական ջանքերը համակարգելու համար, որը գործում է «միասին վերլուծել, գործել իրավասության շրջանակներում» սկզբունքով՝ ինստիտուցիոնալ ինքնուրույնությունը պահպանելու համար:

- Ամբողջ հասարակությանը միտված մոտեցում, որը մոբիլիզացնում է անկախ լրատվամիջոցներին, քաղաքացիական հասարակությանը, ակադեմիական շրջանակներին, տեղական ինքնակառավարման մարմիններին, մասնավոր սեկտորին (ներառյալ հարթակներն ու հեռահաղորդակցության օպերատորները) և համայնքներին՝ մեդիա և թվային գրագիտության, արագ փաստերի ստուգման, միջադեպերի մասին հաղորդելու և ներառական հանրային հաղորդակցության միջոցով դիմակայունությունն ամրապնդելու համար՝ հիմնված առավելագույն թափանցիկության վրա և իրականացվում է իրավունքները, թափանցիկությունը և բազմակարծությունը պաշտպանող եղանակներով:

- Հզոր միջազգային համագործակցության և աջակցության մեխանիզմներ, որոնք ապահովում են աջակցության ընդլայնում, հնարավորություն են տալիս միջսահմանային չեզոքացումներ կատարել և համապատասխանում են ընդհանուր ելակետերին (օրինակ՝ նախագծման միջոցով անվտանգ գործելակերպ, ծագման աղբյուր, որտեղ հնարավոր է, և ժամանակին բացահայտում)՝ ազգային ցանցերը կապելով ավելի լայն «ցանցերի ցանցի» հետ՝ աջակցությունը, համահունչությունը և հաշվետվողականությունը արագացնելու համար:

Զեկույցը գործնական առաջարկություններ է ներկայացնում ընտրական կառավարման մարմիններին, կառավարություններին, քաղաքացիական հասարակության կազմակերպություններին և միջազգային աջակցության դերակատարներին տարբեր ընտրական միջավայրերում՝ սկսած կայացածներից մինչև զարգացող ժողովրդավարություններ: Հիմնական առաջարկությունների թվում են ընտրական մարմինների հզորացումը, գործառնական գերազանցության հասնելը, լավ ռեսուրսներով հագեցած ազգային ընտրական համագործակցության ցանցերի ստեղծումը, հարթակների հաշվետվողականության և քաղաքական գործընթացների ապօրինի ֆինանսավորման վերաբերյալ իրավական շրջանակների կատարելագործումը, ինչպես նաև միջազգային օգնությանը մոդուլային մոտեցման որդեգրումը:

Հիմնական եզրակացությունն այն է, որ շարունակական հիբրիդային հակամարտության դարաշրջանում ընտրական պաշտպանությունը պետք է լինի շարունակական, հարմարվողական, նախաձեռնողական և համագործակցային: Ուժեղ ինստիտուցիոնալ կարողությունների զարգացումը և ամբողջ հասարակությանը ներգրավող մոտեցումը ապահովում են ընտրական գործընթացի անխաթարության ամենաերկարատև պաշտպանությունը:

01 Ներածություն

Եվրոպայի տարբեր ընտրություններում հիբրիդային սպառնալիքները փորձության են ենթարկել ընտրական համակարգերի դիմակայունությունը: Սլովակիայում, 2023 թվականի ընտրություններից ընդամենը երկու օր առաջ, լրատվամիջոցների լռության ժամանակահատվածում տարածվել է արհեստական բանականությամբ ստեղծված ձայնագրություն, որտեղ, ըստ նախնական տեղեկատվության, լիբերալ թեկնածու Միխալ Շիմեչկան և լրագրողը ծրագրում են գնչուական համայնքներից ձայներ գնել: Ռումինիայում, 2024 թվականի նախագահական ընտրությունների նախաշեմին, իշխանությունները բացահայտել են համակարգված հիբրիդային մարտավարություններ՝ սկսած ձայների գնման սխեմաներից, ապատեղեկատվությունից և կիբեռհարձակումներից մինչև ռուսամետ թեկնածուի չհայտարարագրված ֆինանսավորումը: Իսկ Մոլդովայում, 2025 թվականի սեպտեմբերին, նախագահ Մայա Սանդուն զգուշացրեց, որ Մոսկվան խորհրդարանական ընտրություններից առաջ լայնածավալ հիբրիդային պատերազմ է մղում՝ օգտագործելով ապատեղեկատվություն, ընտրակաշառք և - քաղաքական գործընթացների ապօրինի ֆինանսավորման այլ ձևեր, ինչպես նաև ընտրողներին թիրախավորող սպառնալիքի մարտավարություն:[1]

Այս օրինակները միասին ցույց են տալիս, թե ինչպես են ընտրությունները բախվում աճող մարտահրավերների և օտարերկրյա դերակատարների միջամտության հետ, որոնք թիրախավորվում են տեղեկատվական, ֆինանսական և կիբեռոլորտներում համակարգված գործունեությամբ, որը հաճախ նախատեսված է ինստիտուցիոնալ և հասարակական համակարգերի միջև առկա բացերն ու խոցելի կետերը շահագործելու համար:[2] Քանի որ այս սպառնալիքներն անընդհատ զարգանում են, ազատ և արդար ընտրությունները հիբրիդային սպառնալիքներից պաշտպանելը ոչ միայն դարձել է ավելի կարևոր, քան երբևէ, այլև շարունակական և անընդհատ զարգացող մարտահրավեր:[3]

Ժամանակակից սպառնալիքների բնապատկերը ներկայացնում է 20-րդ դարի ավանդական դիվանագիտության և քարոզչության հիմնարար զարգացումը: Թվային ոլորտն այժմ ծանրության կենտրոնն է. հակառակորդները համադրում են կիբեռգործողությունները, դիվերսիոն առցանց տեխնիկան և նարատիվների մանիպուլյացիան. ներքին դերակատարները կարող են գիտակցաբար կամ անգիտակցաբար ուժեղացնել այս ջանքերը: Ռուսաստանի գործողությունները Ուկրաինայի 2014 թվականի ընտրությունների և մասնավորապես 2016 թվականի ԱՄՆ նախագահական ընտրությունների ժամանակ ծառայեցին որպես ջրբաժան պահ՝ բարձրացնելով համաշխարհային իրազեկությունը ժողովրդավարական գործընթացների խոցելիության մասին նման բարդ հիբրիդային սպառնալիքների նկատմամբ:[4]

Կարևորագույն եզրակացությունն այն է, որ ժամանակակից միջամտությունը մեկուսացված գործողությունների շարք չէ, այլ քրոնիկ, պետականորեն աջակցվող տեղեկատվական պատերազմ, որը վարում է գործող անձանց բարդ էկոհամակարգը:[5] Հետախուզական ծառայությունները մշտապես Ռուսաստանին, Չինաստանին և Իրանին են մատնանշում որպես գլխավոր կազմակերպիչներ, որոնք գործում են միջնորդների ցանցի միջոցով՝ պետական լրատվամիջոցներից մինչև հաքերային խմբեր՝ ապահովելու համար հավանական հերքումը:[6] Սահմանն ավելի է մշուշոտվում ներքին քաղաքական խմբավորումների կողմից, որոնք կարող են հանդես գալ որպես օտարերկրյա պատումների գիտակից կամ անգիտակից ուժեղացուցիչներ:[7]

Տեխնոլոգիական առաջընթացը, մասնավորապես արհեստական բանականության ոլորտում, զգալիորեն արագացրել է այս զարգացումը: 2024 թվականից ի վեր գեներատիվ արհեստական բանականության կիրառումը դարձել է ուժի զգալի բազմապատկիչ, որը հնարավորություն է տալիս արագ և ցածր գնով ստեղծել իրատեսական սինթետիկ մեդիա, այդ թվում՝ խորը կեղծիքներ և ձայնային կլոններ, ստեղծել անհատականացված ապատեղեկատվություն արդյունաբերական մասշտաբով, ինչպես նաև ստեղծել չարամիտ արհեստական բանականության խմբերի ներուժ:[8] Թեև արհեստական բանականության կողմից ստեղծված բովանդակության ուղղակի ազդեցությունը ընտրությունների արդյունքների վրա դեռևս դժվար է քանակականացնել, այն ակնհայտորեն ձևավորել է տեղեկատվական միջավայրը և ուժեղացրել առկա կեղծիքների տարածումը:[9] Աշխարհաքաղաքական մրցակցության, առաջադեմ տեխնոլոգիաների և հարմարվողական հակառակորդների այս միաձուլումը սահմանում է ընտրությունները թիրախավորող հիբրիդային սպառնալիքների ներկայիս, բարդ իրականությունը:

1.1. ՀԻԲՐԻԴԱՅԻՆ ՍՊԱՌՆԱԼԻՔՆԵՐԻ ՍԱՀՄԱՆՈՒՄՆ ԸՆՏՐԱԿԱՆ ՀԱՄԱՏԵՔՍՏՈՒՄ

Ընտրությունները թիրախավորող հիբրիդային սպառնալիքները համակարգված, թշնամական գործողություններ են, որոնք համատեղում են ավանդական և ոչ ավանդական միջոցները՝ ժողովրդավարական գործընթացները խարխլելու համար՝ միաժամանակ մնալով զինված հակամարտության շեմից ցածր և հաճախ շահագործելով հայտնաբերման/վերագրման բացերը և պատերազմ-խաղաղություն/ներքին-արտաքին ոլորտների միջև գոյություն ունեցող սահմանները:[10]

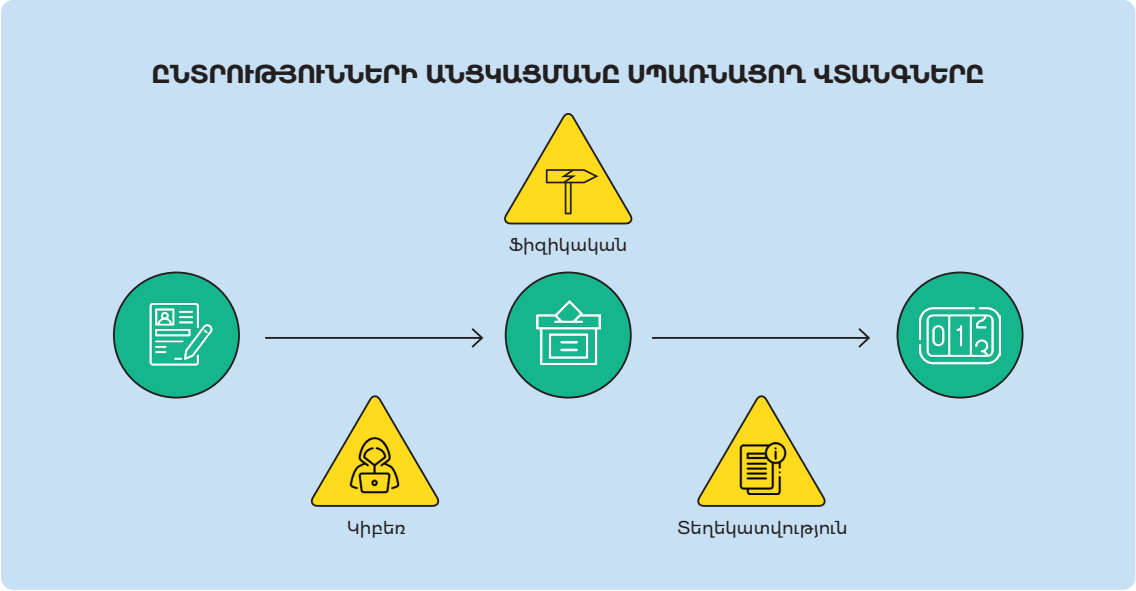
Բեյը (2024) առանձնացնում է ընտրական գործընթացին վերաբերող սպառնալիքների երեք կատեգորիա՝ ընտրությունների անցկացմանը սպառնացող սպառնալիքներ, ընտրությունների նկատմամբ վստահություն և քվեարկելու կամքի և կարողության դեմ պայքար: Այս գործընթացակենտրոն կառուցվածքի հիման վրա այս զեկույցը կիրառում է չորս կատեգորիաներից բաղկացած մոտեցում, որը նաև ներառում է քաղաքական որոշումների կայացումը թիրախավորող սպառնալիքները: Վերլուծական պարզության համար ընտրություններին հատուկ սպառնալիքները խմբավորված են չորս համընկնող կատեգորիաների՝ (ա) ընտրությունների անցկացում, (բ) ընտրությունների նկատմամբ վստահություն, (գ) քվեարկելու կամք/կարողություն և (դ) քաղաքական որոշումների կայացում: Միաժամանակ, այս կատեգորիաներն օգնում են տարբերակել ընտրական գործընթացների խախտումները նախապատվությունները փոխելու կամ լեգիտիմությունը քայքայելու ավելի խորը փորձերից:

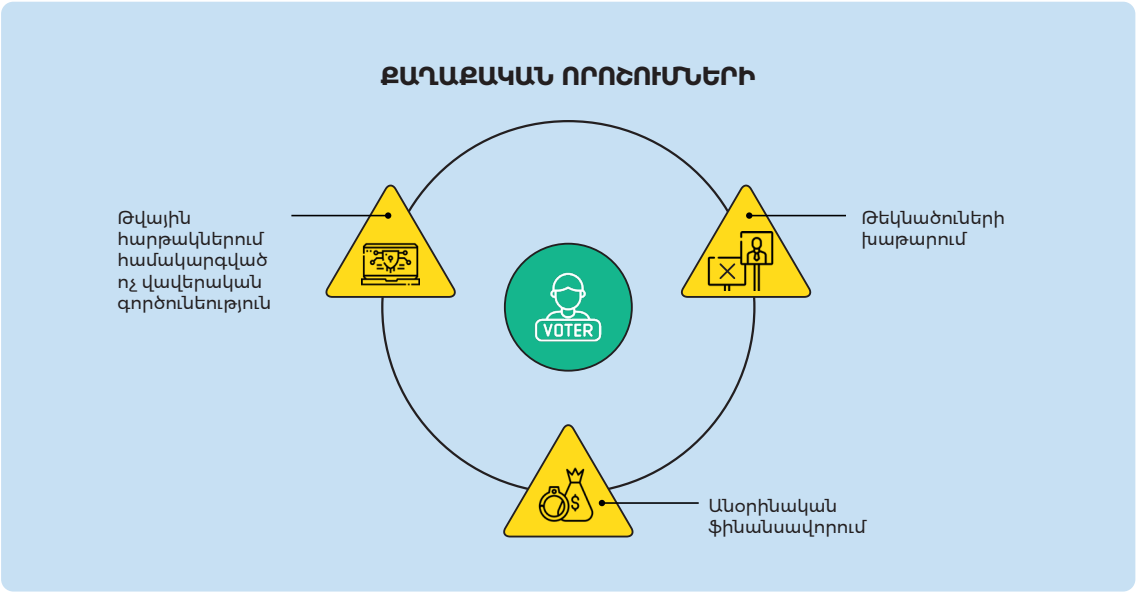
- Ընտրությունների անցկացմանը սպառնացող վտանգները. Գործողություններ, որոնք նպատակ ունեն խաթարել հենց ընտրական գործընթացը՝ թիրախավորելով պաշտոնյաներին, ենթակառուցվածքները կամ լոգիստիկան տեղեկատվական, ֆիզիկական կամ կիբեռմիջոցներով:

- Ընտրությունների նկատմամբ վստահության սպառնալիքներ. Փորձեր, որոնք նպատակաուղղված են ընտրությունների օրինականության հանդեպ հանրության վստահությունը քայքայելու՝ ապատեղեկատվություն տարածելու, դավադրության տեսություններ քարոզելու կամ լայնամասշտաբ խարդախության տպավորություն ստեղծելու միջոցով:

- Քվեարկելու կամքի և կարողության սպառնալիքները. Մեթոդներ, որոնք նախատեսված են ընտրողների վարքագծի վրա ազդելու համար՝ խոչընդոտելով ընտրողների մասնակցությունը կամ խաթարելով նրանց քվեարկելու հնարավորությունը, օրինակ՝ սպառնալիքի կամ կեղծ ընթացակարգային տեղեկատվության տարածման միջոցով:

- Քաղաքական որոշումների կայացման սպառնալիքները. Ընտրողների նախասիրությունների վրա ազդելու փորձեր՝ օգտագործելով անօրինական կամ ոչ լեգիտիմ միջոցներ, ներառյալ թվային հարթակներին կեղծ համակարգված գործունեություն, ապօրինի ֆինանսավորում կամ թեկնածուների խաթարում:





1.2. ԱԶԴԵՑՈՒԹՅՈՒՆՆ ԸՆՏՐԱԿԱՆ ԳՈՐԾԸՆԹԱՑԻ ԱՆԽԱԹԱՐՈՒԹՅԱՆ, ՎՍՏԱՀՈՒԹՅԱՆ ԵՎ ԺՈՂՈՎՐԴԱՎԱՐԱԿԱՆ ԳՈՐԾԸՆԹԱՑՆԵՐԻ ՎՐԱ

Ընտրությունների դեմ հիբրիդային հարձակումների ռազմավարական նպատակը ոչ միայն մեկ ձայնի վրա ազդելն է, այլև ժողովրդավարական էկոհամակարգերի քայքայումը՝ վստահության էրոզիայի, բևեռացման սրման և ժողովրդավարական պետությունների ինստիտուցիոնալ հիմքերի թուլացման միջոցով:[11] Գործնականում սա դրսևորվում է կանոններն ու մրցավարներին կասկածի տակ դնող պատմողական արշավների, խարդախության մասին կազմակերպված պնդումների և լռության ժամանակահատվածներում օրակարգերը ձևավորող ճիշտ ժամանակին արտահոսքերի միջոցով: Պաշտոնյաների արժանահավատությունը վարկաբեկելով, քվեարկության համակարգերի նկատմամբ վստահությունը խաթարելով և սադրիչ ապատեղեկատվություն տարածելով՝ նման արշավները նպատակ ունեն խորացնել բևեռացումը և քայքայել պետության ինստիտուցիոնալ դիմակայունությունը:[12]

> *«Ընտրությունների դեմ հիբրիդային հարձակումների ռազմավարական նպատակը ոչ միայն մեկ ձայնի վրա ազդելն է, այլև ժողովրդավարական էկոհամակարգերի քայքայումը՝ վստահության էրոզիայի, բևեռացման սրման...»*

Չլինելով միակ պատճառը՝ նման սպառնալիքները, հավանաբար, նպաստել են վերջին 15 տարիների ընթացքում ընտրողների միջին մասնակցության համաշխարհային անկմանը մոտ տասը տոկոսային կետով, ինչպես նաև վեճերի աճին, ընդ որում՝ 2020-2024 թվականների միջև ընկած ժամանակահատվածում ազգային ընտրությունների գրեթե յուրաքանչյուր հինգերորդի դեպքում պարտվող կողմը մերժել է արդյունքը:[13]

Վերջին ընտրական ցիկլերը նույնպես ցույց են տալիս շոշափելի հետևանքներ՝ ընտրություններից հետո անկարգություններ և պարտությունը չընդունելու դեպքեր, հաքերային հարձակումների և տվյալների արտահոսքի հետևանքով առաջացած տեղեկատվական ճգնաժամեր, և վարչական խափանումներ, երբ կիբեռմիջադեպերը հետաձգում են ընտրողների գրանցումը կամ արդյունքների հաղորդումը: Մի շարք դեպքերում միջազգային դիտորդները գրանցել են համակարգված ճնշում, որը համատեղում է տեղեկատվական ազդեցության գործունեությունը, ապօրինի ֆինանսավորումը և կիբեռխափանումները, ինչն էլ ավելի է ընդգծում արդեն իսկ բևեռացված միջավայրը:[14]

Այս էրոզիան սրվում է փորձառու ընտրական պաշտոնյաների արտագաղթով, ովքեր բախվում են մշտական հետապնդումների, այդպիսով թուլացնելով ինստիտուցիոնալ կարողությունները:[15] Վերջնարդյունքում ստեղծվում է փակ շրջան. վստահության անկումը մեծացնում է մանիպուլյացիայի նկատմամբ խոցելիությունը, ինչն էլ իր հերթին ավելի է նվազեցնում մասնակցությունն ու համաձայնությունը:[16]

Ավելին, «ընտրակեղծիքների» մասին պատմությունները ունեն կոնկրետ ներքին ազդեցություն՝ առաջացնելով բողոքների և տեղեկատվությանը հասանելիություն ստանալու հարցումների աճ, ճնշում գործադրելով արտահերթ վերահաշվարկների կամ «դատաբժշկական աուդիտների» վրա, ավելացնելով պաշտոնյաների նկատմամբ հետապնդումները և նվազեցնելով ընտրությունների արդյունքները ընդունելու պատրաստակամությունը: Այս պատմությունները տարածվում են նաև սահմաններից այն կողմ, որտեղ նույն շրջանակները հարմարեցվում և վերօգտագործվում են համախոհ ազդեցիկ անձանց և պետական կապակցված լրատվամիջոցների կողմից՝ ձևավորելով սպասումներ քվեարկության օրվանից շատ առաջ:[17]

Ավելին, այս մարտավարությունները մշակված են հասարակական պառակտումները խորացնելու համար: Հակառակորդներն էմոցիոնալորեն լիցքավորված ապատեղեկատվություն են ներմուծում ներգաղթի, տնտեսական քաղաքականության և մշակութային «բաժանարար հարցերի» վերաբերյալ բանավեճերի մեջ՝ նպատակային բևեռացում հրահրելու համար:[18] Մեխանիկորեն, արշավները մեծացնում են սոցիալական ինքնությունների կարևորությունը, քաղաքականությունը ներկայացնում որպես զրոյական գումարով խաղ («մենք ընդդեմ նրանց») և զգացմունքային լիցքավորված պնդումները կապում են անորոշության ժամանակաշրջանների հետ, երբ լսարանն ավելի շատ կախված է խմբային ազդանշաններից և պարզեցված պատմություններից: Այս վիճակում աֆեկտիվ բևեռացումը սրվում է, և ուղղիչ տեղեկատվությունը անտեսվում է:[19]

Այս արշավները հաճախ օգտագործում են մարգինալացված ինքնությունների՝ այդ թվում՝ սեռի, ռասայի և սեռական կողմնորոշման բացասական պատկերումներ՝ սոցիալական պառակտումները մեծացնելու և անհամաչափորեն թիրախավորելու փոքրամասնություններին և կանանց:[20] Օպերատորները նաև միաժամանակ ուժեղացնում են հակադիր կողմերին՝ մարտավարություն, որը հայտնի է որպես «ինքնության կոնվերգենցիա», և շահագործում են միջհատվածային դժգոհությունները, ինչպիսիք են կրոնի և սեռի կամ դասի միջև համընկնումը: Սա մեծացնում է ազդեցության ընդգրկումը և նպաստում է թշնամանքի նորմալացմանը բազմաթիվ համայնքներում:[21]

Սա ինքնահաստատվող շղթայական գործընթաց է առաջացնում. ցածր վստահությամբ բևեռացված հասարակությունը պակաս դիմացկուն է և նույնիսկ ավելի խոցելի ապագա հիբրիդային հարձակումների նկատմամբ: Վստահության անկմանը զուգընթաց՝ խմբային մակարդակում ընկալվող սպառնալիքը մեծանում է, սոցիալական հեռավորությունը մեծանում է, և էլիտաները բախվում են արտակարգ միջոցառումների ճնշմանը՝ պայմաններ, որոնք հակառակորդները վերահաստատում են նոր պատմություններով և ավելի մեծ ազդեցությամբ:[22]

1.3. ԱՇԽԱՐՀԱՔԱՂԱՔԱԿԱՆ ՉԱՓՈՒՄԸ

Ընտրություններին սպառնացող հիբրիդային սպառնալիքները չեն առաջանում մեկուսացված. դրանք սերտորեն կապված են ավելի լայն աշխարհաքաղաքական բնապատկերի հետ: Այս մեթոդների ինտենսիվ օգտագործումը 2024 թվականից սկսվում է ժողովրդավարությունների և ավտորիտար պետությունների միջև ռազմավարական մրցակցությամբ, Ուկրաինայում ընթացող պատերազմով և մի քանի այլ առաջնագծային հակամարտություններով:[23] Ռուսաստանը հաճախ ընտրությունները դիտարկում է որպես հնարավորություններ՝ թուլացնելու Ուկրաինային ցուցաբերվող աջակցությունը, խաթարելու այնպիսի դաշինքներ, ինչպիսիք են Հյուսիսատլանտյան դաշինքի կազմակերպությունը (ՆԱՏՕ) և Եվրամիությունը (ԵՄ), և առաջ մղելու համաշխարհային կարգի վերաձևավորմանն ուղղված վերանայողական օրակարգ:[24]

Այս գործակալների համար տեղեկատվական պատերազմը քաղաքականության հավելում չէ, այլ պետական գործունեության կենտրոնական գործիք, որը վարվում է հետևողական և ասիմետրիկ կերպով:[25]

> Ժողովրդավարական հասարակությունները, որոնք սահմանվում են բաց տեղեկատվական միջավայրերով և խոսքի ազատության նկատմամբ հանձնառությամբ, մարմնավորում են ներքին խոցելիություններ, որոնք հակառակորդները հմտորեն շահագործում են: Ի հակադրություն, ավտորիտար ռեժիմներն օգտվում են փակ, խստորեն վերահսկվող տեղեկատվական էկոհամակարգերից, ինչը նրանց տալիս է զգալի պաշտպանական առավելություն, որը հիմք է հանդիսանում նրանց դիմակայունության համար: Այս գործառնական ասիմետրիան ժամանակակից հակամարտության հիմքում է:[26]

Ուկրաինայում պատերազմը ծառայել է և՛ որպես լաբորատորիա, և՛ որպես կատալիզատոր Ռուսաստանի հիբրիդային սպառնալիքների համար: Արևմտյան ընտրությունների դեմ կիրառված բազմաթիվ մարտավարություններ, տեխնիկա և ընթացակարգեր (և վերջերս լիովին ուժգնությամբ նկատվեցին Մոլդովայում) ուղղակիորեն կապված են Մոսկվայի աշխարհաքաղաքական նպատակների, ինչպես նաև Ուկրաինայի նկատմամբ միջազգային աջակցությունը խաթարելու նրա ռազմավարական նպատակի հետ:[27] Համապատասխանաբար, ընտրությունների պաշտպանությունը այլևս միայն ներքին քաղաքականության հարց չէ. այն անբաժանելի մասն է կազմում միջազգային անվտանգության և ժողովրդավարական մոդելի կոլեկտիվ պաշտպանության, ինչպես բազմիցս ընդգծել են ՆԱՏՕ-ն և Եվրամիությունը:[28]

1.4. ՁԵԿՈՒՅՑԻ ՆՊԱՏԱԿԸ, ԾՐՋԱՆԱԿԸ ԵՎ ՄԵԹՈԴԱԲԱՆՈՒԹՅՈՒՆԸ

Հիբրիդային սպառնալիքների առաջացրած մարտահրավերների կանխարգելումը պահանջում է չարամիտ գործող անձանց կողմից կիրառվող մարտավարության և դրանց հակազդելու համար անհրաժեշտ ռազմավարությունների մանրակրկիտ ըմբռնում: Ծվեդիայի ժողովրդավարության և օրենքի գերակայության ամրապնդման հանձնառության շրջանակներում, Ֆոլկե Բեռնադոտ ակադեմիան (FBA) աջակցում է այս նպատակին՝ հետազոտելով և գիտելիքներով կիսվելով նման սպառնալիքների բախվող միջազգային դերակատարների հետ՝ այդպիսով նպաստելով ավելի դիմակայուն ժողովրդավարությունների զարգացմանը: Այս աջակցությունը տարածվում է ընտրությունների դիտարկումից այն կողմ և ներառում է ընտրությունների աջակցություն՝ ուղղված պատրաստվածության և ընտրական դիմակայունության ամրապնդմանը:

Այս զեկույցը ամփոփում և ներկայացնում է ընտրություններին ուղղված հիբրիդային սպառնալիքների հակազդման վերաբերյալ փորձագիտական գիտելիքներ՝ հիմնական ուշադրությունը կենտրոնացնելով 2024 թվականից ի վեր զարգացումների վրա: Այն սկսվում է ընտրություններին սպառնացող հիբրիդային սպառնալիքների, դրանց ծավալման էկոհամակարգի և ներկայիս համաշխարհային աշխարհաքաղաքական

համատեքստում ընտրական անխաթարության, հանրային վստահության և ժողովրդավարական գործընթացների վրա դրանց ընդհանուր ազդեցության ընդհանուր ակնարկով: Հաջորդ գլուխներում ավելի խորը ուսումնասիրվում են երեք հիմնական ուղիներ, որոնց միջոցով չարամիտ գործող անձինք ազդում են ընտրությունների վրա՝ տեղեկատվության մանիպուլյացիա և միջամտություն, քաղաքական գործընթացների ապօրինի ֆինանսավորում և կիբեռհարձակումներ: Հաջորդում է հիբրիդային սպառնալիքների դեմ պայքարին նվիրված գլուխը՝ հատուկ ուշադրություն դարձնելով ընտրությունների համագործակցության ցանցերի ստեղծման փորձին: Վերջապես, ամփոփիչ գլխում ներկայացված են հիմնական եզրակացություններն ու առաջարկությունները:

Այս զեկույցի հիմնական լսարանը ներառում է ընտրական գործընթացների կազմակերպմանը, աջակցմանը կամ դրանց նպաստմանը ներգրավված հաստատությունները, հատկապես հակամարտություններից տուժած և փխրուն պետություններում, ինչպես նաև հիբրիդային սպառնալիքների ենթարկված երկրներում, մասնավորապես Արևելյան Եվրոպայում և Արևմտյան Բալկաններում, որտեղ FBA-ն առավել ակտիվ է: Հետևաբար, զեկույցը նաև հիմք է հանդիսանում FBA-ի գործնական ծրագրավորման համար՝ այս տարածաշրջաններում ընտրական դերակատարների շրջանում ժողովրդավարական դիմակայունությունը ամրապնդելու համար:

02 Օրարերկրյա տեղեկատվական մանիպուլյացիան և միջամտությունը (FIMI) և ընտրությունները

FIMI-ն ժամանակակից հիբրիդային սպառնալիքների հիմնական բաղադրիչն է՝ ազդեցության բարդ մեխանիզմ, որը նախատեսված է տեղեկատվական միջավայրը աղտոտելու և հասարակական կարծիքը մանիպուլյացիայի ենթարկելու համար: Հաճախ դիտարկվող ռազմավարությունն ինտեգրում է արդյունաբերական մասշտաբի բովանդակության արտադրությունը բազմաշերտ տարածման հետ:[29]

Նախ, հակառակորդները ստեղծում են հսկայական քանակությամբ բովանդակություն՝ հոդվածներից և մեմերից մինչև արհեստական բանականության կողմից ստեղծված խորը ֆեյքեր, որոնք մանրակրկիտ մշակված են՝ շահագործելու հասարակական «բաժանարար խնդիրները», ինչպիսիք են ներգաղթը և տնտեսական անհանգստությունը:[30] Երկրորդ, այս բովանդակությունը տարածվում է մի շարք տեխնիկաների միջոցով, այդ թվում՝ ավտոմատացված բոտերի ցանցերի, համակարգված ոչ իսկական հաշիվների և «ազդեցության վարձույթի» սխեմաների միջոցով, որոնք օգտագործում են վճարովի ազդեցիկ անձանց՝ պետության կողմից հովանավորվող պատմությունները լվանալու

> *«բացահայտում է ռազմավարական մտադրություն, որը տարածվում է ընտրություններին միջամտելուց շատ ավելի հեռու՝ փոխարենը նպատակ ունենալով վարել շարունակական տեղեկատվական պատերազմ»*

համար:[31] Սա հաճախ ներառում է խաբուսիկ ենթակառուցվածքներ, ինչպիսին է «կրկնօրինակ» տեխնիկան՝ օրինական լրատվական կայքերի կլոնավորումը՝ ապատեղեկատվությանը հավաստիություն հաղորդելու համար:[32]

Այս մարտավարական ջանքերն ուղղորդվում են համապարփակ ռազմավարական շրջանակներով: Ռուսական արտահոսած փաստաթղթերը բացահայտում են, որ գործողությունները ղեկավարվում են մանրակրկիտ մշակված «մեթոդիկաներով» (պատմողական ձեռնարկներով), որոնք մանրամասն նկարագրում են, թե ինչպես սրել ներքին լարվածությունը՝ արտաքին քաղաքականության նպատակներն առաջ մղելու համար: Սա բացահայտում է ռազմավարական մտադրություն, որը տարածվում է ընտրություններին միջամտելուց շատ ավելի հեռու՝ փոխարենը նպատակ ունենալով վարել շարունակական տեղեկատվական պատերազմ:[33]

2.1. ՎԵՐՋԻՆ ՄԻՏՈՒՄՆԵՐԸ

2024 թվականի սկզբից ի վեր ժամանակահատվածը տրամադրել է մի շարք խիստ, իրական աշխարհի օրինակների ուսումնասիրություններ, որոնք լուսաբանում են ժողովրդավարական ընտրություններին թիրախավորող հիբրիդային սպառնալիքների զարգացող մարտավարությունը և աճող ինտենսիվությունը: Այս իրադարձությունները, որոնք ընդգրկում են ԵՄ-ն, Միացյալ Նահանգները (ԱՄՆ) և Եվրոպայի արևելյան հարևանությունը, կարևորագույն պատկերացում են տալիս չարամիտ գործողների ներկայիս գործառնական սխեմաների և նրանց կողմից շահագործվող խոցելիությունների մասին:

2024 թվականի Եվրոպական խորհրդարանի ընտրությունները. Միջազգային թիրախ

2024 թվականի հունիսին կայացած Եվրախորհրդարանի ընտրությունները FIMI արշավների համար կարևոր միջազգային թիրախ էին, քանի որ փաստահավաքները հայտնաբերել են ԵՄ-ին ուղղված ապատեղեկատվության կտրուկ աճ առնվազն տասնմեկ երկրներում:[34] Ռուսաստանի սոցիալական դիզայնի գործակալությունը կազմակերպել է «Եվրոպայի դեմ համապարփակ հակաքարոզարշավ», որն ուղղված էր աջ ծայրահեղական և եվրոսկեպտիկ թեկնածուների հզորացմանը՝ տնտեսական կործանման և ազգային արժեքների էրոզիայի պատումներն ուժեղացնելու միջոցով:[35] Այս արշավը մասամբ իրականացվել է ընդարձակ «Doppelgänger» ցանցի միջոցով, որն օգտագործել է կլոնավորված լրատվամիջոցների կայքեր և ստեղծել ազդեցության ցանցեր՝ եվրոպական տեղեկատվական էկոհամակարգում կրեմլամետ ապատեղեկատվություն ներարկելու համար:[36]

Ռումինիայի չեղյալ հայտարարված ընտրությունները. շրջադարձային պահ

Ռումինիայի Սահմանադրական դատարանը, իր ազդեցության դրամատիկ ցուցադրությամբ, չեղյալ հայտարարեց 2024 թվականի վերջին կայացած նախագահական ընտրությունների առաջին փուլի արդյունքները՝ հղում անելով համակարգված արտաքին միջամտությանը և անթափանց առցանց ֆինանսավորմանը: Հետախուզական գործակալությունները բացահայտել են TikTok-ի վրա կենտրոնացած բարդ արշավ, որտեղ վճարովի ազդեցիկ անձանց ցանցերը և լայնածավալ ոչ իսկական գործունեությունը ուժեղացրել են նախկինում մարգինալ, կրեմլամետ թեկնածուի ակտիվությունը, որի առցանց ներկայությունը անհամատեղելի էր հայտարարված քարոզարշավի ծախսերի հետ:[37] ԵՄ մակարդակով հանձնաժողովը նախաձեռնել է «Թվային ծառայությունների մասին» օրենքի (DSA) պաշտոնական ընթացակարգ՝ TikTok-ի վտանգների մեղմացման և Ռումինիայի ընտրությունների հետ կապված առաջարկվող համակարգերի ուսումնասիրության համար:[38]

Վերլուծաբանները բացահայտել են հազարավոր ոչ ակտիվ և առևանգված հաշիվներից բաղկացած ցանց, որոնցից շատերը կապված էին Ռուսաստանի և Իրանի հետ, որոնք ակտիվացվել էին հարթակը մանիպուլյատիվ բովանդակությամբ ողողելու համար: Ինչպես նկարագրված է 3-րդ գլխում, սա զուգորդվել է ապօրինի արտաքին ֆինանսավորման ուժեղ նշաններով, քանի որ թեկնածուի առցանց ներկայությունը շեղվել է պաշտոնապես հայտարարված քարոզարշավի ծախսերից: Մինչ անկախ դիտորդները զգուշության կոչ էին անում՝ նշելով առցանց ակտիվության և քվեարկության միջև ուղղակի պատճառահետևանքային կապը ապացուցելու դժվարությունը, այս դեպքը ցույց է տալիս, թե ինչպես լավ ռեսուրսներով հագեցած FIMI արշավը կարող է խաթարել ընտրությունների արդյունքի նկատմամբ վստահությունը մինչև անվավեր ճանաչելու աստիճան: Միևնույն ժամանակ, Ռումինիայի դեպքը քննադատության արժանացավ, և դիտորդները նշեցին, որ գաղտնի հետախուզական տվյալներին ապավինելը բացեր է ստեղծում թափանցիկության և վիճարկելիության հարցում: Բացի այդ, նրանք պնդում էին, որ համապարփակ միջոցները կարող են չափազանց հեռու գնալ՝ անցնելով վերջնական նպատակից:

Մոլդովայի պայքարը. Ընտրություններ հիբրիդային կրակի ներքո

Մոլդովան իրական ժամանակի օրինակ է ծառայում, թե ինչպես է երկիրը պաշտպանվում ինտենսիվ և ինտեգրված հիբրիդային հարձակումից: Մինչդեռ Ռուսաստանի 2014 թվականի հարձակումը Ուկրաինայի վրա ստեղծեց «հաքերային և հեռարձակող» խաղային սխեման, որը համատեղում է կիբեռներխուժումը

տեղեկատվական մանիպուլյացիայի հետ,[39] Մոլդովայում նրա գործողությունները վերածվել են քրոնիկ, բազմաոլորտային ճնշման, որի նպատակն է երկիրը գրավել քվեատուփերի միջոցով:[40]

Երկրի 2024 թվականի նախագահական ընտրությունները և ԵՄ հանրաքվեն բախվեցին այն բանին, ինչը միջազգային դիտորդները նկարագրեցին որպես արտասահմանից ուղղորդվող «հիբրիդային պատերազմ»:[41] FIMI-ն ծառայեց որպես ինտեգրող շերտ այս բազմադոմենային հարկադրանքի համար: Ռուսաստանի հետ կապված գործիչները պատմություններով լի արշավ էին վարում՝ ԵՄ-ին կողմ կառավարությունը ներկայացնելու որպես անգործունակ, ինչին ուժեղացնում էին համակարգված Telegram ցանցերը և Մոլդովայի ուղղափառ եկեղեցին:[42] Այս տեղեկատվական հարձակումը ֆինանսավորվել է խոշորածավալ անօրինական ֆինանսավորմամբ՝ մոտավորապես 39 միլիոն դոլար, որը փախուստի դիմած օլիգարխից ուղղվել է ընտրակաշառքի և բողոքի ցույցերի ֆինանսավորման համար, և լրացվել է ֆիզիկական խափանումների սպառնալիքներով, ինչպիսիք են սփյուռքի ընտրատեղամասերում կեղծ ռումբի սպառնալիքները:[43]

2024 թվականին կիրառված մարտավարությունը նախերգանք էր 2025 թվականի սեպտեմբերին կայանալիք խորհրդարանական ընտրություններին ուղղված ավելի ինտենսիվ քարոզարշավի: Կրեմլի արտահոսած փաստաթղթերը բացահայտեցին բազմակողմանի ռազմավարություն, որն ուղղված էր Մոլդովայի ԵՄ-ին անդամակցելու ուղին խափանելուն և, ի վերջո, նախագահ Սանդուին իշխանությունից հեռացնելուն:[44] Պլանը մանրամասն նկարագրում էր դասագրքային հիբրիդային սպառնալիքի մոդելը, ներառյալ՝

- Telegram-ի, TikTok-ի և Facebook-ի նման հարթակներում լայնածավալ ապատեղեկատվական արշավ, որն օգտագործում է պատումներ, որոնք նախագահ Սանդուին ներկայացնում են որպես օտարերկրյա խամաճիկ, որը երկիրը պատերազմի է մղում:[45]

- Մեծածավալ ապօրինի ֆինանսավորում՝ ձայներ գնելու և ռուսամետ կուսակցություններին ֆինանսավորելու համար:[46]

- Պաշտոնյաների վրա ճնշում գործադրելու համար կոմպրոմատի (կոմպրոմատի) օգտագործումը և մոլդովական սփյուռքի հավաքագրումը ճանապարհորդելու և քվեարկելու համար:[47]

- Սպորտային ակումբներից և հանցավոր ցանցերից երիտասարդ տղամարդկանց հավաքագրումը՝ բռնի սադրանքներ և խափանող բողոքի ցույցեր կազմակերպելու համար:[48]

Այս պլանն ակտիվորեն կիրառվեց: 2025 թվականի սեպտեմբերի 22-ին՝ ընտրություններից ընդամենը մի քանի օր առաջ, Մոլդովայի իշխանությունները լայնածավալ գործողություն իրականացրին՝ Ռուսաստանի կողմից աջակցվող անկայունացման դավադրությունը կանխելու համար: Ոստիկանությունը ձերբակալել է 74 մարդու և անցկացրել ավելի քան 250 խուզարկություն՝ կոտրելով ցանց, որը, ենթադրաբար, գործում էր Ռուսաստանի ԳՀՎ հետախուզական ծառայության աջակցությամբ և կառավարում էր «Վստահություն» մեդիա խումբը՝ քարոզչություն տարածելու համար:[49] Սա հաջորդեց տեղեկատվական ճակատում ճնշելու ավելի վաղ գործադրված ջանքերին, այդ թվում՝ 443 TikTok ալիք արգելափակելու պաշտոնական խնդրանքին:[50]

Այս գործողությունները լրացվում են մշտական կիբեռճնշմամբ: 2022 թվականից ի վեր ռուսամետ հաքերային խմբերը կիբեռհարձակումներ են իրականացրել կառավարական հաստատությունների վրա, ստեղծել արտահոսքի կայքեր և կոտրել խորհրդարանական էլեկտրոնային փոստի սերվերները՝ հաքերային և արտահոսքի գործողություններին նախապատրաստվելու համար:[51] Այս սրվող սպառնալիքներին ի պատասխան՝ Մոլդովան ստացել է զգալի միջազգային աջակցություն: 2023 թվականին Մոլդովայի Հանրապետությունում ստեղծվեց ԵՄ գործընկերության առաքելությունը (EUPM)՝ Մոլդովայի

հիբրիդային սպառնալիքների, այդ թվում՝ կիբեռանվտանգության և ֆինանսական բռնության դեմ պայքարի միջոցների նկատմամբ դիմակայունությունը բարձրացնելու համար: Բացի այդ, 2025 թվականին Եվրամիությունը Քիշնևում տեղակայեց հիբրիդային արագ արձագանքման խումբ և ԵՄ կիբեռանվտանգության պահուստ՝ ԵՄ կիբեռանվտանգության արագ օգնության մեխանիզմի առաջին ակտիվացումը՝ երկրի ընտրությունների պաշտպանությանը աջակցելու համար:[52]

Ամփոփելով՝ Մոլդովայի դեպքը ցույց է տալիս ժամանակակից ընտրական միջամտության իրականությունը. դա մեկուսացված միջադեպերի շարք չէ, այլ լիովին ինտեգրված հիբրիդային պատերազմ: Սա ընդգծում է պետությունների կողմից միջազգային փորձագիտությունն օգտագործելու, միմյանցից սովորելու և իրենց կարևորագույն ժողովրդավարական համակարգերը ամրապնդելու համար ամբողջ հասարակության պաշտպանություն կառուցելու անհրաժեշտությունը:

Ուկրաինա. Տեղեկատվական պատերազմը որպես ավանդական հակամարտության գործիք

Քանի որ Ուկրաինայում ընտրությունները կասեցված են ռազմական դրության պատճառով, Ռուսաստանի FIMI արշավները Ուկրաինայի դեմ գործում են որպես կանխարգելիչ հարձակում նրա ապագա ժողովրդավարական գործընթացների վրա: Սոցիալական դիզայնի գործակալության «Ուկրաինայի դեմ համապարփակ հակաքարոզարշավը» պատերազմական ջանքերի ուղղակի գործիք է, որն ուղղված է Ուկրաինայի ղեկավարությանը խաթարելուն, նրա զինված ուժերի բարոյալքմանը և սոցիալական համախմբվածության քայքայմանը:[53] Կոռուպցիայի մասին պատմությունները ուժեղացնելով և քաղաքական մրցակցությունը բորբոքելով՝ երկարաժամկետ քարոզարշավը ձգտում է ապահովել, որ պատերազմից հետո ընտրությունների անցկացման ժամանակ ընտրազանգվածը լինի մասնատված և ընկալունակ ռուսամետ այլընտրանքների նկատմամբ:[54]

Ներկայիս ջանքերը զարգացել են նախկին ձեռնարկներից, որոնք կիբեռներխուժումները համատեղում էին տեղեկատվության մանիպուլյացիայի հետ: Ուկրաինայի 2014 թվականի նախագահական ընտրություններից առաջ և ընթացքում Մոսկվային կապված քաղաքական ցանցերը, մեդիա ակտիվները և օլիգարխ միջնորդները մոբիլիզացվել են՝ կրեմլամետ օրակարգերը առաջ մղելու և Ուկրաինայի եվրոպական հետագիծը խոչընդոտելու համար: Ռուսամետ կուսակցություններն ու գործիչները ծառայեցին որպես քաղաքականության համաձայնեցման և ուղերձների տարածման վեկտորներ, մինչդեռ Ռուսաստանի հետ կապված բիզնես շահերը ընդլայնեցին Մոսկվայի լծակները:[55] Զուգահեռաբար՝ կիբեռմիջամտությունը թիրախավորել էր ընտրությունների մեխանիզմները. Կենտրոնական ընտրական հանձնաժողով ներխուժումները ջնջել էին ֆայլեր և տեղադրել կեղծված արդյունքներ ցուցադրելու համար նախատեսված վնասակար ծրագրեր, որոնց լրացել էին DDoS (Distributed Denial-of-Service) հարձակումները՝ հաղորդումը հետաձգելու համար: Ռուսաստանի պետական հեռուստատեսությունը հետագայում հեռարձակեց կեղծ գրաֆիկան՝ կիբեռներխուժումը տեղեկատվական մանիպուլյացիայի հետ համատեղելու վաղ օրինակ:[56] Ուկրաինայում հաջորդ ընտրությունները, կանխատեսվում է, որ տեղի կունենան դժվարին պայմաններում, քանի որ երկիրը, հավանաբար, կբախվի ընտրական գործընթացին ազդելու կամ այն խաթարելու արտաքին փորձերի ուժեղացմանը:

2024 թվականի ԱՄՆ նախագահական ընտրությունները. Բազմադերակատար հարձակում

2024 թվականի ԱՄՆ ընտրությունները կիզակետային կետ էին բազմաթիվ օտարերկրյա դերակատարների համար՝ իրենց տարբեր խաղաոճերով:[57] Ռուսաստանը կիրառեց լայն գործիքակազմ՝ սկսած ընտրատեղամասերում ռումբերի կեղծ սպառնալիքներից մինչև արհեստական բանականության կողմից ստեղծված դիփֆեյքեր, իր «Doppelgänger» ազդեցության ցանցի շարունակական օգտագործումն և ներքին լիազոր ներկայացուցիչների մոբիլիզացումը:[58] Արդարադատության նախարարությունը խափանեց «Doppelgänger» ցանցը՝ առգրավելով 32 դոմեյն և բացահայտելով մեղադրանքները ռուսական պետական

լրատվամիջոցների հետ կապված ռուս գործակալների դեմ:[59] Չինաստանի գործունեությունն ավելի նպատակային էր՝ կենտրոնանալով ԱՄՆ «մշակութային պատերազմի» խզումների և ցածր ձայների մրցավազքի վրա, այլ ոչ թե նախագահական ընտրությունների վրա:[60] Իրանը համատեղեց առցանց հետախուզությունը հաքերային գործողությունների և տվյալների արտահոսքի հետ, ընդ որում՝ ԱՄՆ իշխանությունները մեղադրանք առաջադրեցին Իրանի հետ կապված անձանց՝ նախագահական քարոզարշավին վարկաբեկելու և նյութեր գողանալու նպատակով:[61] Ի պատասխան՝ ԱՄՆ գործակալությունները որդեգրեցին «նախնական սնանկացման» դիրքորոշում և կիրառեցին մեղադրանքների, պատժամիջոցների և առգրավումների համադրություն՝ ծախսերը մեծացնելու և ենթակառուցվածքները խաթարելու համար:[62]

Անկախ գնահատականները նշում են, որ չնայած կուտակային ազդեցության ջանքերը զգալի էին և ավելի ու ավելի շատ հիմնված էին արհեստական բանականության վրա, հիմնական ընտրությունների մեխանիզմի վրա օպերատիվ ազդեցությունը զսպված էր, սակայն տեղեկատվական վնասը (շփոթություն, բևեռացում, ցինիզմ) մնում է որպես կենտրոնական ռիսկ ապագա ցիկլերի համար:[63]

2.2. ՀԱՅԵՏՆԱԲԵՐՄԱՆ, ՎԵՐԱԳՐՄԱՆ ԵՎ ԱՐՁԱԳԱՆՔՄԱՆ ՄԱՐՏԱՀՐԱՎԵՐՆԵՐ

FIMI-ից պաշտպանությունը մի քանի լուրջ մարտահրավերներ է ներկայացնում: Վերագրումը մնում է կարևորագույն խոչընդոտ, քանի որ պրոքսիների և տեղեկատվության լվացման բարդ տեխնիկայի օգտագործումը միտումնավոր նախատեսված է երկիմաստություն ստեղծելու և ժամանակին, համաչափ արձագանքը խոչընդոտելու համար:[64] Արհեստական բանականության միջոցով ուժեղացված ժամանակակից արշավների արագությունն ու մասշտաբները հաճախ գերազանցում են ավանդական հակազդեցություններին, ինչպիսին է փաստերի ստուգումը:[65] Ավելին, ժողովրդավարությունները բախվում են անվտանգության և խոսքի ազատության միջև դժվար հավասարակշռության խնդրի, որը չարամիտ դերակատարներն օգտագործում են՝ պաշտպանական գործողությունները որպես գրաքննություն ներկայացնելով:[66]

Կենտրոնական մարտահրավերը հարթակի հաշվետվողականությունն է, քանի որ շատ սոցիալական մեդիա ընկերությունների բիզնես մոդելները խրախուսում են բևեռացնող բովանդակությունը, որը մեծացնում է ներգրավվածությունը:[67] Վարկանիշային ալգորիթմների, բովանդակության մոդերացիայի կանոնների և հետազոտողների տվյալների հասանելիության վերաբերյալ իմաստալից թափանցիկության ապահովումը շարունակում է մնալ վիճելի կարգավորիչ և քաղաքական մարտահրավեր:[68] ԵՄ DSA-ն ներկայացնում է նշանակալի կարգավորիչ պատասխան, որը պարտավորությունները տեղափոխում է շատ մեծ առցանց հարթակների վրա՝ համակարգային ռիսկերը գնահատելու և թափանցիկությունը բարձրացնելու համար: Կիրարկումը սկսվել է, պաշտոնական ընթացակարգերը կապված են 2024 թվականի ընտրությունների ամբողջականության հետ, սակայն համապատասխանությունը մնում է անհավասար:[69] Ջուգահեռաբար՝ հարթակները վերակարգավորում են իրենց մոտեցումը. Google-ը և Meta-ն հայտարարել են ԵՄ-ում քաղաքական գովազդը սահմանափակելու կամ դադարեցնելու ծրագրերի մասին՝ հղում անելով նոր կարգավորիչ դաշտին:[70]

Մինչ կարգավորումն ուժեղանում է, թափանցիկության այլ ձևերը քայքայվում են: Meta-ի կողմից իր CrowdTangle գործիքի դադարեցումը, որը իրական ժամանակում տեղեկատվություն էր տրամադրում հանրային սոցիալական ցանցերի բովանդակության մասին, նվազեցրեց ազդեցիկ ցանցերի տեսանելիությունը 2024 թվականի խոշոր ընտրություններից առաջ:[71] Արդյունաբերության կամավոր ջանքերը, ինչպիսին է ընտրություններում խաբուսիկ արհեստական բանականությանը հակազդելու «Տեխնոլոգիական համաձայնագիրը», քննադատության են ենթարկվել հաշվետվողականության և չափելի չափանիշների բացակայության համար:[72]

Արհեստական բանականության ծագման և հայտնաբերման շուրջ բացվել է նոր պատասխանատվության ճակատ: Թեև իսկական լրատվամիջոցների պիտակավորման համար ընդունվում են բաց ստանդարտներ, ինչպիսիք են C2PA բովանդակության

հավատարմագրերը, դրանք բախվում են կատվի և մկան դինամիկայի՝ թերի լուսաբանման պատճառով:[73] Զուգահեռաբար, Google DeepMind-ի SynthID-ի նման գործիքները ստեղծման պահին աննկատելի, հուսալի ջրանիշեր են ներդնում անմիջապես արհեստական բանականության կողմից ստեղծված մեդիայի մեջ:[74] Այնուամենայնիվ, նույնիսկ Google-ի սեփական արհեստական բանականության չաթբոտները դեռ չեն ներդրել այս ստանդարտը և դեռևս չեն կարողանում հայտնաբերել իրենց ստեղծած բովանդակությունը: Սա ընդգծում է բովանդակության ծագման համար ուժեղ, փոխգործունակ և պարտադրվող ստանդարտների հրատապ անհրաժեշտությունը:

Քանի որ գեներատիվ արհեստական բանականությունը շարունակում է նվազեցնել ազդեցության գործողությունների ծախսերը, նույնիսկ այն դեպքում, երբ հարթակները ավելացնում են պաշտպանիչ պատնեշներ, այդ գործողությունների նկատմամբ կարգավորիչ վերահսկողության և վերահսկողության պահպանումը կմնա մարտահրավեր:[75] Հետազոտությունները նաև արձանագրել են դեպքեր, երբ պետության հետ կապված կամ պատժամիջոցների ենթարկված կազմակերպությունները կարողացել են գնել կամ տեղադրել ազդեցություն ունեցող բովանդակություն՝ չնայած հարթակի քաղաքականությանը, ինչը ընդգծում է գովազդային տեխնոլոգիաների աուդիտի ենթակա վերահսկողության և պատժամիջոցների ստուգման անհրաժեշտությունը, որոնք գործնականում աշխատում են:[76]

2.3. Ի՞ՆՉ ԿԱՐԵԼԻ Է ԱՆԵԼ: ԸՆՏՐՈՒԹՅՈՒՆՆԵՐԻՆ ԹԻՐԱԽԱՎՈՐՈՂ FIMI-Ի ԴԵՄ ՊԱՅՔԱՐԻ ՌԱԶՄԱՎԱՐՈՒԹՅՈՒՆՆԵՐ

Ընտրական միջամտության էվոլյուցիան դրվագային հարձակումներից դեպի քրոնիկ, համակարգային տեղեկատվական հակամարտության վիճակի պահանջում է պաշտպանական ռազմավարության հիմնարար փոփոխություն: Արհեստական բանականության միջոցով ուժեղացված ժամանակակից FIMI արշավների արագությունն ու մասշտաբները հաճախ գերազանցում են ավանդական հակազդեցություններին, ինչպիսին է ռեակտիվ փաստերի ստուգումը: Հետևաբար, արդյունավետ արձագանքը պետք է լինի նախաձեռնողական, համագործակցային և բազմաշերտ՝ անդրադառնալով սպառնալիքի ինստիտուցիոնալ, կարգավորող և տեխնոլոգիական ասպեկտներին: Կարևոր է, որ FMI-ի հակազդումը պահանջում է հայեցակարգային արձագանք, որը համատեղելի է ժողովրդավարական նորմերի հետ: Եվրոպական Միության կողմից որդեգրված ժամանակակից, իրավունքները հարգող մոտեցումը վարքակենտրոն է: Այն կենտրոնանում է դիտարկելի, մանիպուլյատիվ վարքագծի թիրախավորման վրա, ինչպիսիք են բոտերի ցանցերը կամ համակարգված ոչ իսկական հաշիվները: Սա թույլ է տալիս պետական մարմնին հակազդել թշնամական գործողություններին՝ հիմնվելով ամուր, ապացույցների վրա հիմնված հիմքերի վրա՝ առանց խաթարելու խոսքի ազատությունը:[77]

> *«Կարևոր է, որ FIMI-ի հակազդումը պահանջում է հայեցակարգային արձագանք, որը համատեղելի է ժողովրդավարական նորմերի հետ:»*

Համագործակցության ցանցերի միջոցով կառավարության ամբողջական մոտեցում

Այս զեկույցն ընդգծում է, թե ինչպես են հակառակորդները միտումնավոր շահագործում տարբեր գործակալությունների պարտականությունների միջև եղած խզումները, ինչը մեկուսացված անվտանգության արձագանքը դարձնում է անբավարար: Ընտրությունները թիրախավորող FIMI-ի դեմ պայքարի հիմնարար ռազմավարությունը հավասարապես ինտեգրված և ցանցային պաշտպանության ստեղծումն է, ինչպես դա արվել է մի շարք երկրներում վերջին ընտրությունների ժամանակ (ինչպես մանրամասն նկարագրված է 5-րդ գլխում):

Իրավական և կարգավորող մարմինների ամրապնդման շրջանակներ

FIMI-ի դեմ պայքարի կենտրոնական մարտահրավերը հարթակի հաշվետվողականությունն է: ԵՄ DSA-ն տեղեկատվական միջավայրի կարգավորման առաջատար մոդել է տրամադրում՝ չնայած դրա կիրառելիության վերաբերյալ առկա բանավեճերին: Օրենքը պարտավորություններ է տեղափոխում «շատ խոշոր առցանց հարթակների» վրա՝ գնահատելու ժողովրդավարական գործընթացներին սպառնացող համակարգային վտանգները՝ դրանց առաջարկությունների համակարգերն ավելի թափանցիկ դարձնելու և ստուգված հետազոտողներին տվյալներին հասանելիություն ապահովելու համար: Նման սկզբունքների կիրարկումը կարևորագույն նշանակություն ունի նախագծային մանիպուլյացիաների նկատմամբ պակաս խոցելի տեղեկատվական միջավայր ստեղծելու համար:

Այս կարգավորող մոտեցումը պետք է տարածվի նաև քաղաքական գործընթացների ապօրինի ֆինանսավորման վրա, որը ծառայում է որպես FIMI արշավների ֆինանսավորման հիմնական ուղղություն: Կարևոր է փակել անանուն առցանց նվիրատվությունների, երրորդ կողմի արշավողդների չկարգավորված օգտագործման և սոցիալական ցանցերում գովազդի վրա անթափանց ծախսերի հետ կապված օրենսդրական բացթողումները (ինչպես մանրամասն նկարագրված է 3-րդ գլխում):

Ամբողջ հասարակության դիմակայունության խթանում

Զուտ պետականակենտրոն պաշտպանությունը բավարար չէ, քանի որ երկարաժամկետ ժողովրդավարական դիմակայունությունըկախված է տեղեկացված, քննադատաբար մտածող և ներգրավված հասարակությունից: Հետևաբար, հիմնական ռազմավարություններից մեկը ամբողջ հասարակությանը միտման մեջ ներդրում կատարելն է, որը լիազորում է քաղաքացիներին և ամրապնդում հանրային տեղեկատվական տարածքը զրոյից մինչև վերջ:

Անկախ մեդիա էկոհամակարգերը կարևոր են այս մոտեցման համար: Այնուամենայնիվ, նրանք հաճախ գործում են խիստ սահմանափակումների ներքո՝ ֆինանսական անորոշության, շուկայի կենտրոնացման, քաղաքականացված պետական գովազդի և իրավական կամ ֆիզիկական ճնշման, որոնք սպառնում են թե՛ կայունությանը, թե՛ խմբագրական անկախությանը: Այս մարտահրավերներին դիմակայելը պահանջում է լրացուցիչ ջանքեր:

Մեդիայի և արհեստական բանականության գրագիտության բարձրացման ազգային նախաձեռնությունները կարևոր են քաղաքացիներին մանիպուլյատիվ բովանդակությունը քննադատաբար նույնականացնելու և գնահատելու հմտություններով զինելու համար, այդպիսով ամրապնդելով բնակչության «ճանաչողական պաշտպանությունը»: Սա պետք է լրացվի անկախ լրատվամիջոցների համար ամուր աջակցությամբ, քանի որ բազմազան և լավ ռեսուրսներով հագեցած մեդիա դաշտը կենսականորեն կարևոր պատնեշ է հանդիսանում ապատեղեկատվության դեմ՝ քաղաքացիներին առաջարկելով պետության կողմից հովանավորվող քարոզչությանը հուսալի, փաստերի վրա հիմնված այլընտրանքներ:

Այս աջակցության կարևորագույն տարրը հետաքննական լրագրության մեջ նվիրված ներդրումներն են: Հետաքննչական լրատվամիջոցները բազմիցս ապացուցել են իրենց արդյունավետությունը հիբրիդային սպառնալիքների մեխանիզմների բացահայտման գործում՝ սկսած բարդ անօրինական ֆինանսավորման սխեմաների բացահայտումից և ապատեղեկատվական ցանցերի քարտեզագրումից մինչև հաքերային գործողությունների հետևում կանգնած գործող անձանց բացահայտումը: Նման աշխատանքը կարևոր է ոչ միայն հանրային ըմբռնման, այլև կառավարության պաշտոնական գործողությունների համար անհրաժեշտ ապացույցների բազան ապահովելու համար:

Նախաձեռնողական պաշտպանության և տեխնոլոգիական դիմակայունության կառուցում

Հաշվի առնելով տարածումից հետո ապատեղեկատվությունը վերացնելու դժվարությունը, նախաձեռնողական դիրքորոշումը կարևոր է: Սակայն նպատակը առցանց շրջանառվող յուրաքանչյուր կեղծ պնդման հակազդելը չէ: Ծանրության կենտրոնը գտնվում է արմատական, սովորական թափանցիկության մեջ, որը նվազեցնում է երկիմաստությունը և տրամադրում է ստուգելի փաստեր, որոնց վրա կարող են հույս դնել ուրիշները:[78]

Սա իրականացվում է հանրությանը հասանելի «ճշմարտության աղբյուր» կենտրոնի միջոցով, որը պարունակում է ընթացակարգեր, ՀՏՀ, ուղղումներ և փոփոխությունների գրանցամատյաններ, որը ստանդարտացնում է, թե որտեղ են հանրությունը և լրատվամիջոցները գտնում հեղինակավոր տեղեկատվություն և ստեղծում է կայուն հղման կետ միջադեպերի ժամանակ:[79] Նման գործելակերպը չափելիորեն նվազեցնում է հակառակորդների կողմից շահագործվող տեղեկատվական բացերը և ժամանակի ընթացքում ամրապնդում է հաստատության հեղինակությունը:[80]

Այս թափանցիկության դիրքորոշման շրջանակներում նախնական բացահայտումը կիրառվում է ընտրողաբար և ժամանակային սահմանափակումներով՝ հայտնի ռիսկային պատուհանների (գրանցում, հարցումներ, արդյունքներ) շուրջ՝ մարտավարությունից պաշտպանվելու, այլ ոչ թե յուրաքանչյուր պատմությունը հերքելու համար՝ միաժամանակ նախատեսված լինելով անհավասար ընդունման և ծագման մասին ոչ լիարժեք լուսաբանման համար:[81] Շեշտը դրվում է հակիրճ «ինչ սպասել/ինչպես ստուգել/որտեղ հաղորդել» բացատրությունների վրա, որոնք օգնում են լսարանին ճանաչել մանիպուլյացիայի օրինաչափությունները (օրինակ՝ կեղծ բովանդակություն, կոտրված և արտահոսող շրջանակներ) և ուշադրությունը ուղղել կանոնիկ էջին:[82] Այս կերպ արված դեպքում նախնական դատարկումը թափանցիկության ծախսարդյունավետ արագացուցիչ է, այլ ոչ թե զուգահեռ բովանդակային պատերազմ:[83]

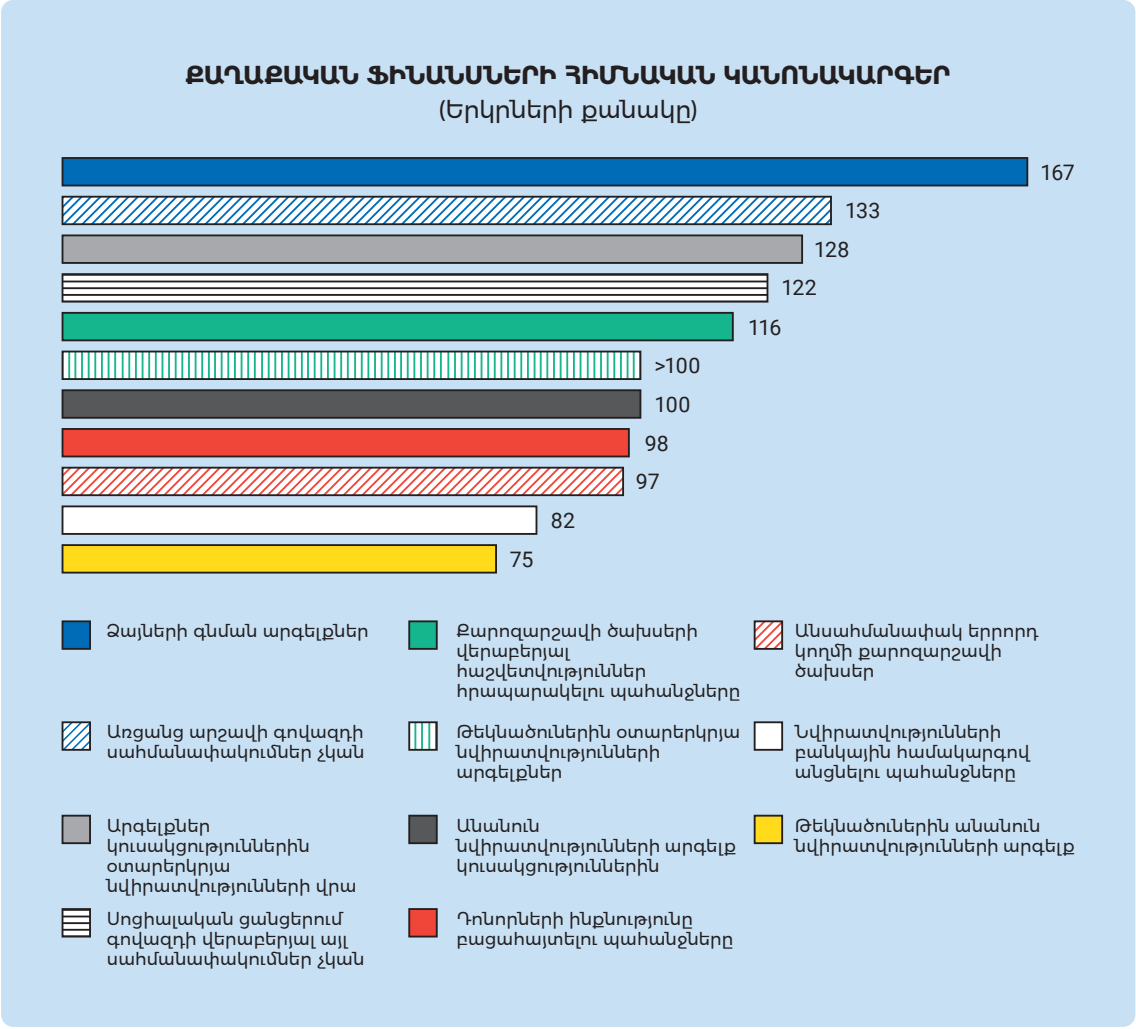
Այս մոտեցումը ճանաչում է սահմանները: Անհնար է հակազդել ապատեղեկատվության յուրաքանչյուր դրսևորման, և մոտիվացված լսարանը երբեմն կնախընտրի համընկնող կեղծիքները: Հետևաբար, ռազմավարությունն այն է, որ ստանանք փաստերը, նեղացնենք անորոշությունը և թիրախավորենք մանիպուլյատիվ վարքագիծը, որպեսզի հավաստի գործող անձինք ունենան կայուն հենարան, որի վրա կարող են հղումներ կատարել, իսկ հանրությունը՝ կանխատեսելի տեղ՝ ստուգելու համար:[84]

Այս թափանցիկության ռազմավարությունը պետք է զուգակցվի տեխնոլոգիական սպառազինությունների մրցավազքի, մասնավորապես՝ արհեստական բանականության կողմից ստեղծված սինթետիկ լրատվամիջոցների մարտահրավերի դեմ պայքարի ծրագրի հետ: Դիփֆեյքերից և ձայնային կլոններից պաշտպանվելը պահանջում է անցնել պարզ

հայտնաբերումից այն կողմ, որը հակառակորդների հետ կապված է «կատվի և մկան դինամիկայի» մեջ:[85] Հեռանկարային ռազմավարությունը բովանդակության ծագման և ջրանիշերի տեխնոլոգիաների մեջ ներդրումներ կատարելն ու դրանց օգտագործումը պարտադրելն է: Բացառապես ստանդարտները, ինչպիսիք են C2PA բովանդակության հավատարմագրերը, որոնք ծառայում են որպես թվային իսկության պիտակ, և հզոր ջրանիշերի գործիքները, ինչպիսին է Google DeepMind-ի SynthID-ը, որը ստեղծման պահին արհեստական բանականության կողմից ստեղծված մեդիայում ներդնում է աննկատելի, մեքենայականորեն հայտնաբերելի ստորագրություն, կարևորագույն նշանակություն ունեն թվային էկոհամակարգում վստահության հիմքը վերականգնելու համար:[86]

Ի վերջո, այս ռազմավարությունները պետք է ինտեգրվեն: Ինչպես եզրակացնում է զեկույցի ընդհանուր եզրակացությունը, ժամանակակից դարաշրջանում ընտրական պաշտպանությունը պետք է լինի շարունակական, հարմարվողական, նախաձեռնողական և համագործակցային գործընթաց:

03 Քաղաքական գործընթացների ապօրինի ֆինանսավորում և հիբրիդային սպառնալիքներ



Դրամն բնույթով քայքայիչ չէ ընտրություններում, այն նաև էական է: Կուսակցությունները դրան են ապավինում գաղափարները առաջ մղելու, անդամներ հավաքագրելու և թեկնածուներ պատրաստելու համար, մինչդեռ ընտրական մարմինները դրա կարիքն ունեն քաղաքացիական կրթության և ընտրությունների լոգիստիկան կառավարելու համար: Այնուամենայնիվ, քաղաքականության մեջ փողը լուրջ ռիսկեր է ներկայացնում ժողովրդավարության համար՝ սկսած ֆինանսավորման անհավասար հասանելիությունից և կոռուպցիոն խթաններից, մինչև ընտրություններին ազդելու նպատակով անօրինական կամ ապօրինի ֆինանսավորում:[87]

Սա ներառում է նաև այն գումարը, որն անօրեն կամ ապօրինի կերպով օգտագործվել է երկրի ներսում և արտերկրում ընտրություններին միջամտելու համար: Վերջինս հատկապես մտահոգիչ է՝ հաշվի առնելով ժողովրդավարական համակարգում դրա առաջացրած աղավաղումները, դրա կողմից առաջացած հանրային վստահության քայքայումը և դրա հետևանքով առաջացող աշխարհաքաղաքական հետևանքները:

Քաղաքական գործընթացների ապօրինի ֆինանսավորման միջոցով արտաքին ընտրական միջամտությունը գնալով ավելի է ճանաչվում, չնայած դա նոր երևույթ չէ: Օրինակ՝ Չեռնոգորիայում 2016 թվականի խորհրդարանական ընտրությունների ժամանակ առաջացան մեղադրանքներ արտաքին քարոզարշավի ֆինանսավորման վերաբերյալ՝ պնդումներով, որ ընդդիմությունը սպասարկում է արտաքին շահերը, մինչդեռ արդեն Մոլդովայի 2021 թվականի վաղաժամկետ ընտրությունների ժամանակ դիտորդները նմանապես մտահոգություններ հայտնեցին արտաքին ֆինանսավորման վերաբերյալ:[88]

3.1. ՔԱՂԱՔԱԿԱՆ ԳՈՐԾԸՆԹԱՑՆԵՐԻ ԱՊՕՐԻՆԻ ՖԻՆԱՆՍԱՎՈՐՈՒՄԸ ՈՐՊԵՍ ՄԻՋԱՄՏՈՒԹՅԱՆ ԳՈՐԾՈՆ

Կան երեք կարևոր ոլորտներ, որոնց միջոցով չարամիտ դերակատարները սովորաբար փորձում են ազդել ընտրությունների վրա՝ քաղաքական գործընթացների ապօրինի ֆինանսավորման միջոցով: Դրանք ներառում են՝ (1) ընտրակաշառք, (2) օտարերկրյա և անանուն նվիրատվություններ, այդ թվում՝ կրիպտոարժույթների միջոցով, և (3) երրորդ կողմի նվիրատվություններ, սոցիալական ցանցերում գովազդի և ազդեցիկ անձանց ֆինանսավորում:

Ձայների գնում

Չնայած արգելված է 167 երկրներում, ձայների գնումը մնում է ընտրություններին ազդելու տարածված միջոց:[89] Մոլդովայի 2025 թվականի խորհրդարանական ընտրությունների ժամանակ միջազգային դիտորդները նշեցին, թե որքանով են բացահայտվել ընտրողների վրա ազդելուն ուղղված ձայների գնման սխեմաներ, և այդ ջանքերը համակարգվել են Ռուսաստանի կողմից ֆինանսավորվող կազմակերպված ցանցի կողմից:[90]

Երկիրը նմանատիպ մարտահրավերների էր բախվել նախորդ ընտրությունների ժամանակ: Օրինակ՝ 2023 թվականի տեղական ինքնակառավարման մարմինների ընտրություններում Ռուսաստանի հետ կապված քաղաքական գործակալները մեղադրվեցին երկիր միջոցներ ուղղորդելու փորձի մեջ՝ ձայներ գնելու նպատակով, այդպիսով նպաստելով ռուսական շահերին:[91] Վատն այն է, որ 2024 թվականի նախագահական ընտրությունների և սահմանադրական հանրաքվեի ժամանակ միջազգային դիտորդները նշել են, թե ինչպես են իրավապահ մարմինները, բազմաթիվ միջազգային գործակալներ և քաղաքացիական հասարակությունները Մոլդովան նկարագրել որպես ընթացիկ «հիբրիդ պատերազմի» թիրախ, որը ներառում է քաղաքական գործընթացների ապօրինի ֆինանսավորում, դեզինֆորմացիա և կիբեռրահարձակումներ:[92]

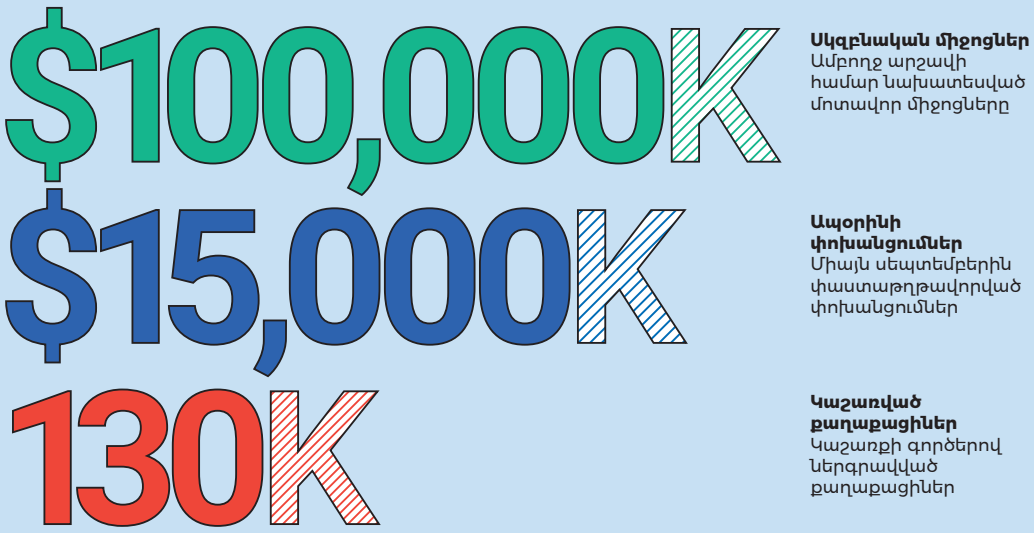
Ենթադրվում է, որ այս սխեմաները ներառել են կանխիկ քարտերի տարածում Ռուսաստանում: Վերլուծաբանները ենթադրյալ գործելաոճը նկարագրել են հետևյալ կերպ.

Ըստ որոշ տեղեկությունների՝ փախուստի դիմած, ԱՄՆ-ի կողմից պատժամիջոցների ենթարկված օլիգարխ Իլան Շորի հետ կապված անձինք երկիր են ներմուծել մաքսանենգ ճանապարհով միլիոնավոր դոլարներ՝ շրջանցելով իրավապահ մարմինների ջանքերը՝ կանխելու միջոցների անօրինական հոսքը: Իշխանությունները խուզարկություններ էին կազմակերպել օդանավակայանում՝ կանխելու համար գաղտնի կանխիկ գումար վերադարձնելու նպատակով Մոսկվա մեկնող այս անձանց շքերթը: Սակայն Ռուսաստանը գտել է այլ եղանակներ՝ Մոլդովա միջոցներ ուղղորդելու համար: Ռուսական MIR վճարային համակարգի միջոցով, ըստ տեղեկությունների, ֆինանսական ռեսուրսները ուղղվում են մոլդովացի ընտրողներին, մասնավորապես՝ Մերձդնեստրի տարածաշրջանի տնտեսական ցանցերի միջոցով՝ անջատողական տարածք, որը երկար ժամանակ ծառայել է որպես Մոսկվայի ազդեցության գործողությունների բազա:

Մոլդովայի իշխանություններն ահազանգ են հնչեցրել մեծածավալ ընտրակաշառքի վերաբերյալ, ընդ որում՝ ոստիկանության գլխավոր տեսչությունը միայն սեպտեմբերին փաստաթղթավորել է կաշառակերության դեպքեր, որոնցում ներգրավված են եղել առնվազն 130,000 քաղաքացիներ և Ռուսաստանից ապօրինի փոխանցումների ավելի քան տասնհինգ միլիոն դոլար: Իրականում, մասշտաբները կարող են զգալիորեն ավելի մեծ լինել, որոշ պաշտոնյաներ այն գնահատում են մոտ 100 միլիոն դոլար ամբողջ քարոզարշավի համար:

Միջոցները ուղղվում են ազգային ձայների գնման ցանց ստեղծելու համար նախատեսված սխեմաների, որոնք նման են ֆինանսական բուրգերի՝ գործարքների բարդ շերտերով, որոնք ուղղված են ստուգումից խուսափելուն: Այս միջոցները տատանվում են մոլդովացի թոշակառուների համար նախատեսված «սոցիալական» նպաստներից մինչև Գագաուզիայի ինքնավար տարածքի տեղական ինքնակառավարման մարմինների աշխատակիցների աշխատավարձի «բոնուսներ»: Ոստիկանության և անկախ լրատվամիջոցների տվյալներով՝ այդ գումարը այժմ նաև հայտնվում է «Հաղթանակ» ընտրական դաշինքի այսպես կոչված տեղական «համակարգողների» և «աջակիցների» ձեռքում, որը քաղաքական միավոր է, որը ստեղծվել է Մոսկվայում և, ըստ որոշ տեղեկությունների, վերահսկվում է Մոսկվայից (Olari 2024):

ՌՈՒՍԱԿԱՆ ԴՐԱՄԱԿԱՆ ՄԻՋՈՑՆԵՐԸ ՀՈՍՈՒՄ ԵՆ ԴԵՊԻ ՄՈԼԴՈՎԱ



Սկզբնական միջոցներ
Ամբողջ արշավի համար նախատեսված մոտավոր միջոցները

Ապօրինի փոխանցումներ
Միայն սեպտեմբերին փաստաթղթավորված փոխանցումներ

Կաշառված քաղաքացիներ
Կաշառքի գործերով ներգրավված քաղաքացիներ

Արտասահմանյան և անանուն նվիրատվություններ

Արտասահմանյան և անանուն նվիրատվությունների արգելքները կամ սահմանափակումները քաղաքական գործընթացների ֆինանսավորման ամենատարածված կարգավորումներից են: 2025 թվականի դրությամբ 128 երկիր արգելում է կուսակցություններին օտարերկրյա նվիրատվությունները, իսկ ավելի քան 100 երկիր արգելքը տարածում է թեկնածուների վրա: Անանուն նվիրատվությունները նույնպես սահմանափակված են 100 երկրներում՝ կուսակցությունների և 75 երկրներում՝ թեկնածուների համար:[93]

Արտասահմանյան նվիրատվությունների արգելքը, ընդհանուր առմամբ, հիմնված է այն սկզբունքի վրա, որ արտաքին շահերը չպետք է ազդեն ազգային քաղաքականության վրա: Ի հակադրություն, անանուն նվիրատվությունների արգելքը սովորաբար նպատակ ունի արգելափակել այլապես անօրինական նվիրատվությունները: Այնուամենայնիվ, այս կանոնների կիրառումը վերահսկող մարմինների համար ամենաբարդ խնդիրներից մեկն է: Ընտրություններին միջամտելու համար կատարված օտարերկրյա նվիրատվությունները կարող են մեծ մասամբ աննկատ անցնել սահմաններից այն կողմ, հաճախ անցնելով արտասահմանյան իրավասությունների և հարկային դրախտների միջով, որտեղ դրանց իրական աղբյուրը հեշտությամբ թաքցվում է: Սա չափազանց դժվարացնում է միջոցների հետքը գտնելը և դրանց օտարերկրյա ծագումը վերջնականապես պարզելը:[94]

Կրիպտոարժույթները ավելի են բարդացնում իրավիճակը՝ հնարավորություն տալով անթափանց ֆինանսական հոսքերի, այդ թվում՝ արտասահմանում ընտրությունների վրա ազդել ձգտող հակառակորդ դերակատարների կողմից: Վերջին տասնամյակում դրանց օգտագործումն արագորեն ընդլայնվել է. չնայած Bitcoin-ը շարունակում է գերիշխող դիրք գբաղեցնել, ավելի քան 16,000 կրիպտոարժույթ այժմ առևտրվում է ավելի քան 1300 բորսաներում, որոնց օգտատերերի թիվը ամբողջ աշխարհում գնահատվում է 861 միլիոն՝ կազմելով աշխարհի բնակչության մոտ 11 տոկոսը՝ ավելի քան 150 երկրներում:[95] Ավելին, կանխատեսվում է, որ շուկան կշարունակի աճել, և կրիպտո առևտրի արժեքը 2025 թվականի 71.35 միլիարդ ԱՄՆ դոլարից կաճի մինչև 2032 թվականը գերազանցող 260 միլիարդ ԱՄՆ դոլար:[96]

Քաղաքական ֆինանսավորումը անմիջականորեն տուժել է, քանի որ կրիպտոարժույթային գործարքների մեծ մասի անանունությունը հատկապես դժվարացնում է օտարերկրյա նվիրատվությունների հետագծումը:[97] Նշանակալի օրինակ էին 2016 թվականի ԱՄՆ նախագահական ընտրությունները, երբ մեծ ժյուրիի մեղադրական եզրակացությունը բացահայտեց, որ ռուսական միջոցները ենթադրաբար ուղղորդվել են կրիպտոարժույթային բորսաների միջոցով:[98] Դեպքը ընդգծեց վերահսկողության սահմանափակումները՝ ցույց տալով, որ նույնիսկ համեմատաբար ամուր պաշտպանություն ունեցող համակարգը դժվարանում էր լուծել կրիպտոարժույթների խնդիրը, քանի որ օրենսդրությունը թույլ էր տալիս քաղաքական կոմիտեներին ընդունել նվիրատվություններ՝ միաժամանակ ձեռնարկելով միայն «նվազագույն ինտրուզիվ» քայլեր դոնորների քաղաքացիությունը ստուգելու համար:

Երրորդ կողմի ներդրումներ, սոցիալական մեդիա գովազդի ֆինանսավորում և ազդեցիկ անձինք

Երրորդ կողմի ծախսերը կարող են ծառայել որպես արտասահմանյան միջոցների ուղի, որոնք նախատեսված են ընտրություններին ազդելու համար, իսկ կազմակերպությունները կամ անհատները, այդ թվում՝ կեղծ ընկերությունները, ՀԿ-ները կամ բարեգործական կազմակերպությունները, գործում են որպես ճակատային կազմակերպություններ, քարոզարշավ են անցկացնում կուսակցությունների և թեկնածուների օգտին կամ դեմ և դառնում են արտաքին ազդեցության խողովակներ:[99]

Սոցիալական ցանցերում գովազդը դրամահավաքի և քաղաքական գործողությունների մեկ այլ հզոր գործիք է, քանի որ թվային քարոզարշավների ծախսերը կտրուկ աճում են ամբողջ աշխարհում, մասնավորապես COVID-19 համավարակից հետո:[100] Առցանց մեդիա գովազդը օտարերկրյա դերակատարներին հնարավորություն է տալիս միջամտել ընտրություններին,

ինչը հնարավոր է դառնում գովազդի աղբյուրների և դրանց թիրախների միջև ֆիզիկական հեռավորության, ինչպես նաև միկրոթիրախավորում իրականացնելու և ստեղծված բովանդակությունը անհատականացնելու հնարավորության շնորհիվ:[101] Օրինակ, օտարերկրյա դերակատարը կարող է սոցիալական մեդիայի հաղորդագրությունների ծառայություններ գնել որևէ արշավի անունից՝ ներքին վերահսկողության հասանելիությունից դուրս, մինչդեռ առցանց վճարումների անթափանցիկությունը թույլ է տալիս դոնորներին մնալ անանուն:[102]

2018 թվականի Cambridge Analytica սկանդալը վաղ օրինակ է ծառայում, որը վերաբերում է 2016 թվականի ԱՄՆ ընտրությունների ժամանակ Facebook-ի ավելի քան 50 միլիոն օգտատիրոջ անձնական տվյալների չարաշահմանը: Այն նաև բացահայտեց տասնյակ օտարերկրյա քաղաքացիների անօրինական զբաղվածությունը, որոնց քարոզարշավի հաղորդագրությունների, տվյալների վերլուծության և գովազդի վրա կատարված աշխատանքը համարվեց անօրինական բնեղեն օտարերկրյա ներդրում:[103]

2024 թվականի ԱՄՆ ընտրությունները մեկ այլ օրինակ են բերում: «Կրկնօրինակ օպերացայի» շրջանակներում Արդարադատության նախարարությունը առգրավել է Ռուսաստանի կառավարության կողմից չարամիտ ազդեցության արշավների համար օգտագործվող 32 ինտերնետային դոմեյն: Հետաքննության համաձայն՝ գործողությունը հիմնված էր վճարովի ազդեցիկ անձանց, վճարովի սոցիալական ցանցերում գովազդների, որոնցից մի քանիսը ստեղծվել էին արհեստական բանականության կողմից, և կեղծ սոցիալական ցանցերի էջերի օգտագործման վրա, որոնք ներկայանում էին որպես ԱՄՆ կամ այլ ոչ ռուս քաղաքացիներ, որպեսզի օգտատերերին ուղղորդեին կիբեռզավթված կայքեր, որոնք քողարկված էին որպես օրինական լրատվամիջոցներ:[104]

Նույն թվականին Ռումինիայի ընտրությունները ցույց տվեցին նմանատիպ միտումներ, որոնք, ի վերջո, հանգեցրին դրանց չեղյալ հայտարարմանը: Մեկ թեկնածու հայտնել է քարոզարշավի որևէ ծախսի մասին, չնայած լայն առցանց ներկայությանը և հետախուզական տվյալներին, որոնք ենթադրում էին արտաքին աղբյուրներից չհայտարարագրված ֆինանսավորում: Դեպքը ընդգծեց ռազմավարական կոռուպցիայի ավելի լայն ռիսկերը, այդ թվում՝ երրորդ կողմի ֆինանսավորումը լիազորված անձանց միջոցով՝ թվային գովազդը ֆինանսավորելու համար՝ առանց բացահայտելու դրանց ծագումը կամ պահպանելու իրավական առաստաղները, հիբրիդային քաղաքական ֆինանսավորման պատերազմը, որը մեծացնում է արտասահմանից առցանց ճանաչելիությունը, և ընտրական մարմինների կողմից թույլ վերահսկողությունը, որոնք ի վիճակի չեն հետևել բարդ թվային գովազդային ցանցերին:[105]

Վերջերս, Լեհաստանի՝ 2025 թվականի նախագահական ընտրությունների երկրորդ փուլի ժամանակ, միջազգային դիտորդները հայտնել են Facebook-ի կասկածելի արտասահմանյան ֆինանսավորմամբ գովազդների մասին: Ապրիլի կեսերից մինչև մայիսի կեսերը երկու նոր էջ մոտ 500,000 զլոտի (139,000 ԱՄՆ դոլար) են ծախսել մեկ թեկնածուին աջակցող և մյուսներին հարձակվող ավելի քան 100 տեսագովազդների վրա՝ գերազանցելով թեկնածուների ծախսը: Գործը, որը հայտարարվել է որպես հավանական օտարերկրյա ֆինանսավորում, դեռևս քննության տակ է: Դիտորդները քննադատեցին իշխանությունների ուշացած արձագանքը, մինչդեռ Meta-ն հայտարարեց, որ գովազդները չեն խախտում իր չափորոշիչները կամ ազգային օրենսդրությունը: Պարզվել է, որ մեկ այլ հաշվի վրա տեղադրվել է 388,000 զլոտի (մոտավորապես 108,000 ԱՄՆ դոլար) արժողությամբ գովազդներ՝ ենթադրաբար օգտագործելով քաղաքացիական հասարակության կազմակերպության միջոցով արտասահմանից փոխանցված միջոցները: Եվ չնայած Ազգային ընտրական հանձնաժողով և դատախազություն բողոքներ են ներկայացվել ենթադրյալ անօրինական օտարերկրյա ֆինանսավորման վերաբերյալ, դիտորդները նշել են, որ «մինչդեռ Meta-ն ավտոմատացված գործընթացի միջոցով սահմանափակումներ է կիրառում գովազդատուների նկատմամբ ծախսերի նկատմամբ, սոցիալական հարթակի կողմից ներքին կանոնների կիրառումը դուրս է քարոզարշավի ֆինանսավորման վերահսկող մարմնի ներկայիս շրջանակներից և կարողություններից»:[106] Այս դեպքը ընդգծում է արտասահմանյան ֆինանսավորմամբ առցանց քարոզարշավի կողմից ազգային վերահսկողության մեխանիզմների առջև ծառացած աճող մարտահրավերը, ինչպես նաև թվային քաղաքական գովազդի թափանցիկությունն ու հաշվետվողականությունն ապահովելու գործում գործող կարգավորող շրջանակների սահմանափակումները:

3.2. Ի՞ՆՉ ԿԱՐԵԼԻ Է ԱՆԵԼ: ՔԱՂԱՔԱԿԱՆ ԳՈՐԾԸՆԹԱՑՆԵՐԻ ՖԻՆԱՆՍԱՎՈՐՄԱՆ ԿԱՐԳԱՎՈՐՄԱՆ ԵՎ ԱՐՏԱՔԻՆ ՄԻՋԱՄՏՈՒԹՅԱՆ ԴԵՄ ՎԵՐԱՀՍԿՈՂՈՒԹՅԱՆ ԱՄՐԱՊՆԴՄԱՆ ՌԱԶՄԱՎԱՐՈՒԹՅՈՒՆՆԵՐ

Հաշվի առնելով վերը նշված բազմաթիվ մարտահրավերները, պե՞տք է արդյոք արձագանքը կենտրոնանա ավելի խիստ քաղաքական ֆինանսավորման կանոնակարգեր սահմանելու, թե՞ վերահսկողության ուժեղացման վրա:

Խստացնող կանոնակարգեր

Տիպիկ արձագանքը նվիրատվությունների սահմանաչափի իջեցումն է և քարոզարշավի ծախսերի սահմանափակումը: Թեև երբեմն անհրաժեշտ և նույնիսկ ցանկալի է, չափազանց սահմանափակումները կարող են նոր անհավասարակշռություններ ստեղծել և, ի վերջո, ազդել ընտրությունների արդյունքի վրա: Ինչպես արդեն նշվել է, կուսակցություններին և թեկնածուներին անհրաժեշտ են օրինական միջոցներ՝ իրենց գործունեությունը միջամտությունից զերծ իրականացնելու համար: Առանց այդ միջոցների նրանք կարող են դիմել թաքնված արտաքին աջակցության կամ թերագնահատել եկամուտներն ու ծախսերը:[107]

Այնուամենայնիվ, ընտրություններին ուղղված հիբրիդային սպառնալիքները կանխելու և մեղմելու համար հաճախ անհրաժեշտ են ավելի խիստ կարգավորումներ, չնայած նման միջոցառումները պետք է ուշադիր մշակվեն՝ ապահովելու համար, որ հակազդեցության ջանքերն իրենք չառաջացնեն նոր աղավաղումներ կամ սահմանափակումներ, որոնք խաթարում են ժողովրդավարական հիմնական սկզբունքները:

Արգելքներ և սահմանափակումներ

Կարևոր քայլ է կուսակցություններին և թեկնածուներին օտարերկրյա և անանուն նվիրատվությունների արգելումը, այն դեպքերում, երբ դրանք դեռևս արգելված չեն:[108] Կանոնակարգերը կարող են նաև կատարելագործվել՝ համապատասխանեցնելով հաշվետվությունների ժամանակահատվածները իրական քարոզարշավի ժամանակացույցին՝ փոխարենը հույսը դնելու արհեստական կամ նեղ սահմանված հաշվետվությունների ժամանակահատվածների վրա, որոնք բացառում են իրական քարոզարշավի մեծ մասը, երբ արտաքին միջամտության ռիսկը, թերևս, ամենակարևորն է: Եկամուտների և ծախսերի միջև անհամապատասխանությունների բացահայտումը կարող է օգնել բացահայտել անօրինական ֆինանսավորման աղբյուրները:

Ընտրություններում արտաքին միջամտության վերահսկման մեկ այլ մարտահրավեր է երրորդ կողմերի օգտագործումը քարոզարշավի ծախսերը ուղղորդելու համար, մի պրակտիկա, որը դեռևս անսահմանափակ է 97 երկրներում:[109] Սոցիալական ցանցերում գովազդը լուրջ բացթողում է. 133 երկիր սահմանափակումներ չի դնում առցանց քարոզարշավների գովազդի վրա, իսկ 122-ը՝ այլ սահմանափակումներ չի կիրառում: Հետևաբար, օտարերկրյա ազդեցության զսպումը պահանջում է առցանց քաղաքական գովազդի ավելի ուժեղ կարգավորում, ներառյալ թվային քարոզարշավի ավելի ճշգրիտ սահմանումները և թափանցիկության ավելի մեծ պահանջները:[110]

Միջազգային համաձայնեցում

Մեկ այլ առաջնահերթություն է իրավասությունների միջև կարգավորումների ամրապնդումը և միջազգային նորմերի ու մեխանիզմների առաջխաղացումը՝ միջազգային ֆինանսական հոսքերի թափանցիկությունը բարելավելու համար: Սա կարևոր է, քանի որ անօրինական քաղաքական ֆինանսավորումը հաճախ տեղաշարժվում է հարկային դրախտների և օֆշորային կառույցների միջով՝ իր ծագումը թաքցնելու համար: Այս շրջանակների կենտրոնական դերը խաղում է Ֆինանսական գործողությունների աշխատանքային խումբը և դրա փողերի լվացման դեմ պայքարի չափորոշիչները, մասնավորապես՝ քաղաքականապես ազդեցիկ անձանց և օֆշորային իրավասություններին վերաբերողները:[111]

Ընտրություններին սպառնացող հիբրիդային սպառնալիքներին անդրադառնալը նաև պահանջում է ավելի հստակ կանոններ քաղաքական ֆինանսներում կրիպտոարժույթի օգտագործման վերաբերյալ՝ հաշվի առնելով դրա անանունությունը և հստակ կարգավորման բացակայությունը: Հսկողությունը հաճախ բարդանում է դրանց իրավական կարգավիճակի վերաբերյալ պարզության բացակայության պատճառով՝ արդյոք դրանք համարվում են ակտիվներ, արժեթղթեր, թե՞ ֆիաթ արժույթ, և, դրա հետ կապված, դրամական և բնեղեն ներդրումների իրավական տարբեր վերաբերմունքի պատճառով: Համակարգերի մեծ մասում կրիպտոարժույթները համարվում են ակտիվներ և, հետևաբար, դիտվում են որպես բնեղեն նվիրատվություններ, սակայն դա միշտ չէ, որ այդպես է, ինչը մոնիթորինգային գործակալությունների համար ավելի դժվար է դարձնում կիրառելի իրավական շրջանակի որոշումը և դրանց հետևումը:[112]

Ի պատասխան, որոշ երկրներ սահմանափակել կամ ամբողջությամբ արգելել են կրիպտոարժույթների օգտագործումը քաղաքական ֆինանսներում՝ համապատասխանեցնելով օտարերկրյա և անանուն նվիրատվությունների վերաբերյալ ավելի լայն սահմանափակումներին: Օրինակ՝ Իռլանդիան 2022 թվականին ընդունեց օրենք, որն արգելում է կուսակցություններին կրիպտոարժույթներով նվիրատվությունները:[113] Նման միջոցառումները հատկապես արդիական են այն կրիպտոարժույթների համար, որոնք բնույթով անանուն են, որոնց թվում են ամենատարածվածներից մի քանիսը:[114] Կրիպտոարժույթների օգտագործումը սահմանափակելու և քաղաքական ֆինանսների հետ կապված ռիսկերը մեղմելու մեկ այլ (անուղղակի) միջոց է պահանջել, որ նվիրատվությունները անցնեն բանկային համակարգով, ինչպես դա տեղի է ունենում 82 երկրներում:[115]

Պետական վերահսկողության բարելավում

Կանոնակարգերի խստացումից ավելի կարևոր է արդեն իսկ գործողների կիրառումը: Այնուամենայնիվ, վերահսկողությունը մնում է ամենաթույլ օղակը, որտեղ գործակալությունները հաճախ խոչընդոտվում են անորոշ մանդատների, սահմանափակ կարողությունների և վատ համակարգման պատճառով: Սա հատկապես կարևոր է ընտրական մարմինների և ֆինանսական հետախուզության ստորաբաժանումների միջև անհրաժեշտ համագործակցության առումով, հաշվի առնելով վերջիններիս արտոնյալ հասանելիությունը քաղաքական ֆինանսավորման հոսքերի մոնիթորինգի համար անհրաժեշտ հիմնական տեղեկատվությանը:[116]

> *«Կանոնակարգերի խստացումից ավելի կարևոր է արդեն իսկ գործողների կիրառումը:»*

Ավելի ուժեղ կարողություններն ու համագործակցությունը կենսականորեն կարևոր են կրիպտոարժույթային գործարքները վերահսկող մարմինների համար, մասնավորապես՝ վիրտուալ արժույթի փոխանակիչների հետ համագործակցության համար: Որպես ֆինանսական միջնորդներ, այս դերակատարները կարող են տրամադրել կարևոր տեղեկատվություն օտարերկրյա դոնորներին նույնականացնելու համար, և որոշ իրավասություններում արդեն իսկ պարտավորված են փողերի լվացման դեմ պայքարի կանոններով:[117] Նույնքան կարևոր է վերահսկողության համակարգը հագեցնել առցանց գովազդի ծախսերը վերահսկելու ավելի լավ կարողություններով:[118]

Հատկանշական է, որ պետական և ոչ պետական վերահսկողության միջև փոխհարաբերությունները փոխադարձաբար ամրապնդվում են: Երբ իշխանությունները տեղեկատվությունը հրապարակում են անհապաղ և մատչելի ձևով, քաղաքացիական հասարակությունը կարող է ավելի լավ ուսումնասիրել հայտարարագրված ծախսերը՝ համեմատած իր սեփական մոնիթորինգի հետ:[119] Չնայած, որ երկրների մեծ մասը հրապարակում է նման զեկույցներ (116), ավելի քիչ երկրներ (98) են պահանջում դոնորների

ինքնության բացահայտում: Վերջինս կենսականորեն կարևոր բաղադրիչ է կուսակցությունների կամ թեկնածուների ֆինանսավորման միջոցով ընտրությունների վրա ազդել ձգտող օտարերկրյա դերակատարների բացահայտման համար:[120]

Քաղաքացիական հասարակության և լրատվամիջոցների մոնիթորինգի ամրապնդում

Քաղաքացիական հասարակությունը, լրագրողները և բացահայտողները կենսական դեր են խաղում քաղաքական գործընթացների ապօրինի ֆինանսավորումը բացահայտելու գործում, հատկապես, երբ դրանք կապված են ընտրություններին ազդել ձգտող օտարերկրյա չարամիտ դերակատարների հետ: Այնուամենայնիվ, վերջին տարիներին լրատվամիջոցների ազատությունն ու ամբողջականությունը վատթարացել են, քանի որ «Ժողովրդավարության տեսակների ինստիտուտը» հաղորդել է, որ 2024 թվականին 44 երկրներում գրաքննությունը աճել է, իսկ լրագրողներին ուղղված սպառնալիքները՝ ավելացել:[121] Այս միտումը նկատելի է նաև Եվրոպայում, որտեղ թվային հսկողությունը, ապատեղեկատվությունը և հանրային լրատվամիջոցների վրա քաղաքական ազդեցությունը նպաստել են անկմանը:[122]

Ավելի լայն առումով, քաղաքացիական հասարակության դերակատարները բախվում են մի շարք մարտահրավերների, այդ թվում՝ տեղեկատվության և ռեսուրսների սահմանափակ հասանելիության, քաղաքական ճնշման և քաղաքացիական տարածքի սահմանափակման: Այս գործոնները սահմանափակում են նրանց կարողությունը արդյունավետորեն կատարելու իրենց վերահսկողի դերը:[123] Սա ընդգծում է իշխանությունների կողմից ինչպես ամուր թափանցիկության, այնպես էլ անկախ վերահսկողության պաշտպանության, տեղեկատվության հասանելիության երաշխիքների, SLAPP-ի դեմ պայքարի միջոցառումների, պետական գովազդային շուկաներին արդար մուտքի և հետազոտողների համար անվտանգ ուղիների անհրաժեշտությունը:[124]

Կարևոր է նաև նշել, որ լրատվամիջոցներն իրենք կարող են լինել արտաքին միջամտության թիրախ (տե՛ս 3-րդ բաժինը՝ FIMI-ի և ընտրությունների վերաբերյալ): Նման դեպքերում լրատվամիջոցները կարող են ոչ միայն ձախողվել քաղաքական գործընթացների ապօրինի ֆինանսավորման վերահսկողական իրենց դերում, այլև դառնալ սխալ տեղեկատվության և ապատեղեկատվության խողովակներ:[125]

04 Կիբեռանվտան-գության ընկրություններում

Թվային ոլորտը շարունակում է մնալ ընտրական միջամտության կարևորագույն և խիստ վիճարկելի վեկտոր: Կիբեռգործողությունները հազվադեպ են լինում մեկուսացված իրադարձություններ. փոխարենը, դրանք հաճախ ինտեգրվում են ավելի լայն հիբրիդային սպառնալիքների արշավների մեջ՝ հաճախ ծառայելով որպես տեղեկատվության մանիպուլյացիայի և հոգեբանական գործողությունների հիմնական խթանիչ: Սպառնալիքները կարելի է լայնորեն բաժանել երկու կատեգորիայի՝ թիրախավորել են հիմնական ընտրական ենթակառուցվածքները, և թիրախավորել են քարոզարշավները, կուսակցությունները և գործընթացին ներգրավված պաշտոնյաներին:

2024 թվականից ի վեր ժամանակահատվածը նշանավորվել է երկու փոխակերպող միտումներով՝ պետության կողմից հովանավորվող գործողությունների միաձուլումը կիբեռհանցագործության էկոհամակարգի հետ և արհեստական բանականության ի հայտ գալը որպես չարամիտ գործակալների համար հզոր ուժի բազմապատկիչ:[126] Այս միաձուլումը հանգեցրել է սպառնալիքների բարդության և փոխկապակցվածության աճի՝ մշուշելով լրտեսության, խափանումների և շահույթ հետապնդող հանցագործության միջև սահմանները, այդպիսով պահանջելով կիբեռանվտանգության դիմակայունության շարունակական ամրապնդում:[127]

4.1. ՍՊԱՌՆԱԼԻՔՆԵՐԻ ՉԱՐԳԱՑՈՂ ՊԱՏԿԵՐԸ. ՍՊԱՌՆԱԼԻՔՆԵՐԻ ՄԻԱՀՅՈՒՍՈՒՄ, ԱՌԵՎՏՐԱՅՆԱՑՈՒՄ ԵՎ ԱՐՀԵՍՏԱԿԱՆ ԲԱՆԱԿԱՆՈՒԹՅՈՒՆ

Կիբեռսպառնալիքների միջավայրում տեղի ունեցող մակրո մակարդակի փոփոխություններն են ձևավորում ընտրությունների անվտանգության ներկայիս մարտահրավերները: Վերլուծությունը չպետք է սահմանափակվի սպառնալիքների պարզապես ցանկագրմամբ, այլ պետք է բացատրի այն խորքային գործընթացները, որոնց հետևանքով հակառակորդները դառնում են ավելի կարողունակ, հարմարվող և դժվար հակազդելի:

Կիբեռհանցագործությունը որպես ծառայություն (CaaS) էկոհամակարգը. Ռազմավարական համակեցություն

Պետական հովանավորությամբ ստեղծված շարունակական թիրախային հարձակումների (APT) և ֆինանսապես մոտիվացված կիբեռհանցագործների միջև ավանդական տարբերությունը թուլանում է, թեև չի վերանում: Տարիներ շարունակ մտահոգություններ են հնչել կազմակերպված հանցավորության հետ կապվող կիբեռհարձակումների քաղաքական օգտագործման վերաբերյալ, օրինակ՝ սկանդալներով բացահայտվել է լրագրողներին լրտեսելու համար ցանցերի ստեղծումը:[128] Եվրոպոլի կողմից վերջերս անցկացված ուսումնասիրությունն ավելի է ընդգծում պետության կողմից հովանավորվող գործողությունների և կազմակերպված հանցավորության միջև սահմանների մշուշոտ լինելը, որտեղ հանցավոր խմբավորումներն օգտագործվում են իրենց տեխնիկական հմտությունների և ենթակառուցվածքների համար:[129]

Սա հանգեցրել է կիբեռհանցագործությունը որպես ծառայություն (CaaS) մասնագիտացված շուկայի ստեղծմանը, որը օգնում է պետության հետ կապ ունեցող դերակատարներին՝ տրամադրելով մասնագիտացված հնարավորություններ և ստեղծելով կապի «հավանական

ժխտելիության» լրացուցիչ շերտ:[130] Այս ծառայությունները ավելի ու ավելի են օգտագործվում աշխարհաքաղաքական դրդապատճառներով իրականացվող արշավներում՝ թույլ տալով պետական դերակատարներին ուժեղացնել իրենց կարողությունները, իրականացնել խափանիչ հարձակումներ և մասնակցել բարդացված տեղեկատվական ազդեցության գործողություններում:[131]

Ի՞նչ է իրականում փոխվում: Սպառնալիքների միահյուսումը արտացոլում է երկու համընկնող դինամիկա՝[132]

- Արտապատվիրակում կապը հերքելու նպատակով համար. Պետությունները հանձնարարում, հնարավորություն են տալիս կամ հանդուրժում են քրեական և միջնորդ (պրոքսի) դերակատարներին՝ ստեղծելով տարանջատման լրացուցիչ շերտեր և բարդացնելով վերագրումը:

- Շուկայի կողմից թելադրված կարողությունների ընդլայնում. Քրեական էկոհամակարգերն այժմ առաջարկում են APT-ին հարակից գործիքներ «որպես ծառայություն»՝ նվազեցնելով ծախսերը և արագացնելով գործողությունների իրականացումը՝ առանց փոխելու պետությունների հիմնական ռազմավարական նպատակները:

Ըստ էության, սա ոչ թե պետության մտադրության դոկտրինալ փոփոխություն է, այլ գործառնական էվոլյուցիա, որն ընդլայնում է հավանական հերքման և արագ ընդլայնման կարողությունը:[133]

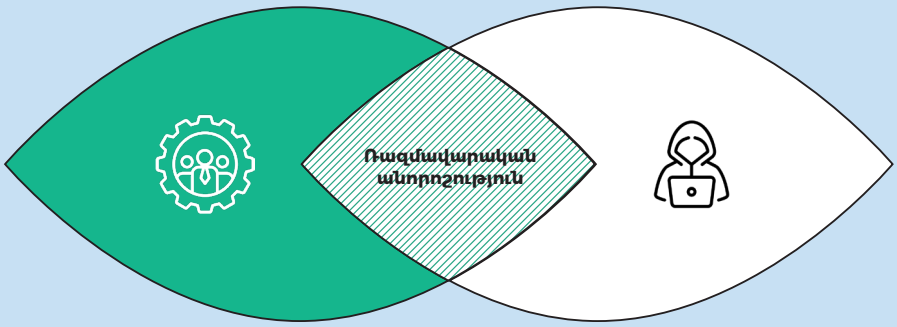
Պետական դերակատարները, մասնավորապես՝ Ռուսաստանը, Չինաստանը և Իրանը, մշտապես նշվում են որպես կարևորագույն ենթակառուցվածքների, այդ թվում՝ ընտրական համակարգերի համար հիմնական արտաքին սպառնալիքներ:[134] Նրանք այժմ կարող են օգտագործել այս CaaS էկոհամակարգը՝ զգալի ազդեցություն ունենալով: Օրինակ՝ 2024 թվականի հուլիս և օգոստոս ամիսներին, ԱՄՆ ընտրությունների ցիկլի ընթացքում, ReliaQuest-ը՝ կիբեռանվտանգության ընկերությունը, որը մասնագիտացած է սպառնալիքների հայտնաբերման և միջադեպերին արձագանքման մեջ, հետաքննել է համակարգված ֆիշինգային արշավ, որը ներկայացել է ակտիվիստական խմբի անվան տակ: Էլ.փոստերով կոչ էին անում թիրախներին «ստորագրել խնդրագիր» և հղումները նրանց վերահասցեավորում էին դեպի որոշակի վնասակար ծրագրերի ցանցի հետ կապված ենթակառուցվածքներ: Նպատակը օգտատերերին սեղմման միջոցով ներգրավելն էր և կոտրված կայքերում «drive-by» տեխնիկական ակտիվացնելը, որը սովորաբար կեղծ զննարկչի թարմացման հուշումներ է տալիս՝ ի վերջո տեղադրելով հեռակա մուտքի տրոյական ծրագիր կամ հավաքելով մուտքային տվյալները:[135] Այս դեպքը ցույց է տալիս էկոհամակարգին բնորոշ գործելաոճը և պատասխանատվության փոխանցման շղթաները, բայց ինքնին չի վկայում պետության կողմից ուղղորդման մասին:

Այս պետական-հանցավոր համակեցությունը ժամանակակից հիբրիդային պատերազմի միտումնավոր առանձնահատկություն է, որը նախատեսված է զսպումը և վերագրումը բարդացնելու համար: Երբ պետական դերակատարը գործում է հանցավոր լիազորված անձի միջոցով, դա ստեղծում է ռազմավարական անորոշություն: Հարձակումը կարող է սկսվել հայտնի փրկագին պահանջող խմբի կողմից, բայց ուղղորդվել, հնարավոր լինել կամ հանդուրժվել պետական հետախուզական ծառայության կողմից: Սա հեշտությամբ կաթվածահար է անում ավանդական արձագանքման մեխանիզմները: Անհասկանալի է դառնում՝ միջադեպը իրավապահ մարմինների տիրույթում է՝ հանցավոր խմբավորմանը հետապնդելու համար, թե՞ ազգային անվտանգության մարմինների՝ թշնամական պետությանը զսպելու նպատակով: Այս անորոշությունը հովանավոր պետությանը հնարավորություն է տալիս հերքելու և դանդաղեցնում է համակարգված արձագանքի համար անհրաժեշտ միջազգային կոնսենսուսը, այդպիսով առավելագույնի հասցնելով գործողության կործանարար ազդեցությունը:[136]

Քաղաքականության տեսանկյունից հետևությունն այն է, որ արձագանքները պետք է համադրեն վարքագծի վրա հիմնված չափորոշիչներ՝ նախ գործելով վնասի և ցուցիչների հիման վրա, ինչպես նաև ունենան՝վերագրման հստակ չափորոշիչներ և իրավական հստակ

ընթացակարգային ուղիներ, որոնք ապահովում են պատշաճ իրավական ընթացակարգի երաշխիքները՝ միաժամանակ հնարավորություն տալով ժամանակին պաշտպանական գործողություններ ձեռնարկելու:

ՀԻԲՐԻԴԱՅԻՆ ՊԱՏԵՐԱԶՄԻ ԵՐԿԻՄԱՍՏՈՒԹՅԱՆ ԳՈՏԻՆ



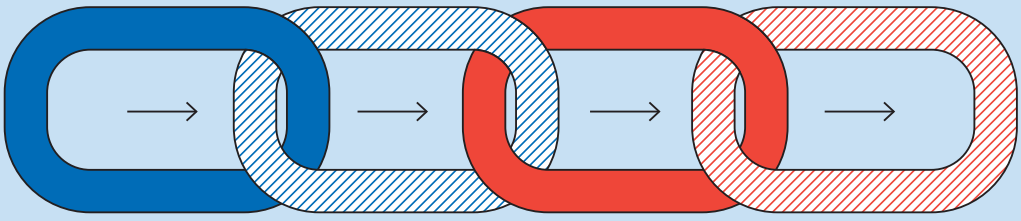
Պետական դերակատարներ
Կառավարության կողմից ղեկավարվող հետախուզական գործողություններ

Քրեական միջնորդներ
Փրկագին պահանջող խմբեր և կիբեռհանցավորության խմբեր

Արհեստական բանականությունը որպես չարամիտ ուժի բազմապատկիչ. հարձակողական և պաշտպանական նպատակով օգտագործումներ

ԱՄՆ կիբեռանվտանգության և ենթակառուցվածքների անվտանգության գործակալությունը (CISA) գնահատել է, որ 2024-2025 թվականների ժամանակահատվածում գեներատիվ արհեստական բանականությունը չի ավելացրել ռիսկերի լիովին նոր կատեգորիաներ, այլ զգալիորեն ուժեղացրել է արդեն իսկ գոյություն ունեցողները:[137] Սակայն արհեստական բանականությունն օգտագործվում է սոցիալական ինժեներիայի հարձակումների մասշտաբը, արագությունը և բարդությունը մեծացնելու համար: Սա ներառում է ավելի հղկված, համատեքստը հաշվի առնող ֆիշինգային էլեկտրոնային նամակների ստեղծում, չափազանց իրատեսական կեղծ պատկերների և դիփֆեյք տեսանյութերի ստեղծում, ինչպես նաև սոցիալական ցանցերի կեղծ պրոֆիլների ստեղծում՝ ազդեցության գործողություններին աջակցելու համար:[138]

ԱՐՀԵՍՏԱԿԱՆ ԲԱՆԱԿԱՆՈՒԹՅԱՆ ՄԻՋՈՑՈՎ ՀԶՈՐԱՑՎԱԾ ՇՂԹԱ



Արհեստական բանականությունը բարձրացնում է խայծի որակը
Արհեստական բանականությունը բարելավում է ֆիշինգի խայծերը NLP-ի և անհատականացված բովանդակության միջոցով

Մուտքի տվյալների գողություն
Զոհերը մուտքագրում են իրենց տվյալները կեղծ մուտքի էջերում

Կողմնային շարժում
Հարձակվողները ցանցում տեղաշարժվում են գողացված մուտքային տվյալներով

Տվյալների արտահոսք/ գործառնությունների խափանում
Հարձակվողները գողանում են տվյալներ կամ խաթարում գործողությունները

Միևնույն ժամանակ, նույն արհեստական բանականության տեխնիկաներից շատերը կիրառվում են պաշտպանական նպատակներով, ինչպիսիք են անոմալիաների հայտնաբերումը, տեսակավորումը և ավտոմատ կերպով նշագրված ֆիշինգի հերթերը, ինչը ընդգծում է, որ տեխնոլոգիան ինքնին խնդիրը չէ: Փոխարենը, մրցակցությունը կայանում է կիրառման որակի, կառավարման և հարձակողական ու պաշտպանական կիրառությունների միջև զարգացող սպառազինությունների մրցավազքի մեջ:

2023-ից 2025 թվականներին կիբեռանվտանգության Hoxhunt ընկերության կողմից անցկացված լայնորեն մեջբերվող փորձը փորձարարորեն ցույց տվեց այս էվոլյուցիան: 2025 թվականի սկզբին նրանց արհեստական բանականությամբ աշխատող ֆիշինգային գործակալը 24 տոկոսով ավելի արդյունավետ դարձավ օգտատերերին խաբելու հարցում, քան էլիտար մարդկային կարմիր թիմերը, այսինքն՝ լիազորված փորձարկողները, որոնք ընդօրինակում են իրական հարձակվողներին՝ թույլ կողմերը բացահայտելու համար:[139] Թեև արդյունքները կարող են տարբեր լինել՝ կախված կազմակերպությունից և վերապատրաստման մակարդակից, սա ցույց է տալիս, որ արհեստական բանականությունն այժմ կարող է ստեղծել գերազանց թիրախային ֆիշինգային հարձակումներ՝ արդյունավետորեն նվազեցնելով այն հնարավորությունների արգելքները, որոնք մի ժամանակ կապված էին ամենաառաջադեմ հակառակորդների հետ:

2024 թվականի ուսումնասիրություններն արդեն ցույց են տվել խորը կեղծ (դիթֆեյք) աուդիո և վիդեո նյութերի օգտագործումը բարձր ռիսկային ֆինանսական խարդախության մեջ, այդ թվում՝ մի միջադեպ, որի արդյունքում մի ընկերությունից խաբեությամբ կորցվեց 25 միլիոն ԱՄՆ դոլար, ինչը ցույց է տալիս տեխնոլոգիայի հասունությունը խաբուսիկ նպատակներով, որոնք կարող են վերաօգտագործվել կամ հարմարեցվել քաղաքական նպատակների համար:[140] Այնուամենայնիվ, մեծ կորուստներով առանձին դեպքերը չպետք է չափազանց ընդհանրացնել բոլոր ընտրական համատեքստերի համար:

Այս տեխնոլոգիական տեղաշարժը խորը հետևանքներ ունի ընտրությունների անվտանգության համար, քանի որ այն արդյունավետորեն նվազեցնում է մեծ բարդության հարձակումներ իրականացնելու մուտքի արգելքը: Ավելի քիչ հմուտ դերակատարներն այժմ կարող են ստեղծել խիստ համոզիչ, անհատականացված թիրախային ֆիշինգային բովանդակություն, որը նախկինում լավ ռեսուրսներ ունեցող APT-ների տիրույթն էր: Այս զարգացումը մեծացնում է սպառնալիքների թե՛ ծավալը, թե՛ ընդհանուր որակը: Ֆիշինգային էլ.փոստերի դասական ցուցիչները, ինչպիսիք են վատ քերականությունը կամ ընդհանուր ողջույնները, այժմ հաճախ վերացվում են արհեստական բանականության կողմից:

Սա մարդակենտրոն պաշտպանությունները, ինչպիսին է օգտագործողի իրազեկման նպատակով վերապատրաստումը, դարձնում է անհրաժեշտ, բայց զգալիորեն ավելի դժվար և պակաս հուսալի: Անվտանգության թիմերը և ընտրական գործընթացների ամենօրյա աշխատողները այժմ բախվում են ավելի մեծ մարտահրավերի, քանի որ հնարավոր խախտումների ծավալն ու որակը մեծացնում են հաջող հարձակման հավանականությունը:

Սա անհրաժեշտ է դարձնում պաշտպանական ռազմավարության անցումը շերտավոր տեխնիկական վերահսկողությանը, որն ավելի քիչ է հիմնված մարդկային դատողության և ավելի շատ զրոյական վստահության ենթակառուցվածքի վրա, որտեղ յուրաքանչյուր օգտատեր և սարք անընդհատ ստուգվում է՝ աջակցվող ուժեղ տեխնիկական պաշտպանությամբ: Դրանք ներառում են ֆիշինգին դիմացկուն բազմագործոն նույնականացում և նվազագույն արտոնություններով ու պայմանական մուտք, որոնք օգտատերերին տրամադրում են միայն անհրաժեշտ նվազագույն մուտքը և միայն որոշակի պայմաններում:

Այն նաև ենթադրում է OAuth համաձայնության կառավարում, այսինքն՝ այն բանի ուշադիր կառավարում, թե որ արտաքին հավելվածները կարող են միանալ հիմնական համակարգերին, ինչպես նաև կցումների և հղումների մեկուսացում, որի միջոցով պոտենցիալ ռիսկային բովանդակությունը բացվում է անվտանգ, կարանտինային միջավայրերում: Ծրագրերի թույլատրված ցուցակագրումը մեկ այլ կարևոր միջոց է, որը թույլ է տալիս գործարկել միայն հաստատված ծրագրակազմը, ինչպես նաև մակրոների արգելափակումը, որը անջատում է փաստաթղթերում ավտոմատացված կոդը:

Այլ միջոցառումներից են սարքերի համապատասխանությունը և հավաստագրումը՝ ապահովելով, որ բոլոր միացված սարքերը համապատասխանեն անվտանգության չափանիշներին, ինչպես նաև ժամանակին կառավարումը, որը ադմինիստրատորի իրավունքներ է տալիս միայն անհրաժեշտ կարճ ժամանակահատվածում, և կարևորագույն գործընթացների խելամիտ ֆիզիկական տարանջատումը՝ ամենազգայուն համակարգերը պահելով անջատված կամ առանձնացված ցանցերում: Հնարավորության դեպքում, այս վերահսկողությունները պետք է զուգակցվեն միջադեպերի մասին հաղորդագրությունների արդյունավետ համակարգի և հստակ հաղորդակցման արձանագրությունների հետ՝ հետագա տեղեկատվության ազդեցությունը զսպելու համար:[141]

4.2. ԸՆՏՐԱԿԱՆ ԿԱՐԵՎՈՐԱԳՈՒՅՆ ԵՆԹԱԿԱՌՈՒՑՎԱԾՔՆԵՐԻՆ (ՑԱՆՑԵՐ, ՏՎՅԱԼՆԵՐԻ ԲԱԶԱՆԵՐ ԵՎ ՔՎԵԱՐԿՈՒԹՅԱՆ ՏԵԽՆՈԼՈԳԻԱՆԵՐ) ՍՊԱՌՆԱՑՈՂ ՎՏԱՆԳՆԵՐ

Ընտրությունների տեխնիկական ենթակառուցվածքը. ներառյալ ամեն ինչ՝ սկսած ընտրողների գրանցման տվյալների բազաներից մինչև պաշտոնական արդյունքների հրապարման կայքերը. մնում է չարամիտ գործակալների հիմնական թիրախը: Թեև քվեարկության սարքերի ուղղակի մանիպուլյացիան՝ ձայների հաշվարկը փոխելու նպատակով, լայնորեն համարվում է դժվար իրականացվելիք այնպիսի մասշտաբով, որ չհայտնաբերեն, մասնավորապես այն համակարգերում, որտեղ գործում են թղթային հուսալի վերահաշվարկի մեխանիզմներ, այնուամենայնիվ դրանց շրջակա ենթակառուցվածքը ներկայացնում է բազմաթիվ խոցելիություններ:[142]

Վերջին տարիներին դիտարկվող աչքի ընկնող մարտավարություններից մեկը բաշխված ծառայությունների մերժման (DDoS) հարձակումների կիրառումն է: Սրանք նախատեսված են ընտրական կայքերը և ընտրողների տեղեկատվական պորտալները ավելորդ բովանդակությամբ ծանրաբեռնելու համար, ինչը դրանք անհասանելի կդարձնի: Փրկագին պահանջող հարձակումները ևս մեկ լուրջ սպառնալիք են ներկայացնում: Կարևորագույն համակարգերը կոդավորելով և դրանց թողարկման համար վճար պահանջելով՝ այս հարձակումները կարող են լուրջ խափանումներ առաջացնել:[143]

Ընտրական համակարգերի խախտումներ

Ընտրական տվյալների բազաների խախտումները հատկապես նենգ սպառնալիք են ներկայացնում, քանի որ դրանք կարող են անմիջապես չխաթարել ծառայությունները, բայց կարող են խաթարել հանրային վստահությունը: Ցանկացած խախտում՝ իրական կամ ենթադրյալ, կարող է օգտագործվել FIMI-ի արշավներում՝ ընտրական գործընթացի նկատմամբ հանրության վստահությունը խաթարելու համար:[144] 2023 թվականին պարզվեց, որ Մեծ Բրիտանիայի ընտրական հանձնաժողովը հաքերային հարձակման է ենթարկվել, հավանաբար, պետության հետ կապված անձի կողմից, որի արդյունքում վտանգվել են մոտ 40 միլիոն ընտրողների տվյալները: 2024 թվականին հարձակումը, որը վերագրվեց Չինաստանի հետ կապված խմբի, ամիսներ շարունակ աննկատ մնաց: Չնայած պաշտոնյաները հայտարարեցին, որ դա չի ազդել քվեարկության կամ ձայների հաշվարկի վրա, ընտրողների այդքան մեծ ցուցակի բացահայտումը ընդգծում է այն հետախուզական արժեքը, որը հակառակորդները տեսնում են ընտրությունների տվյալներում:[145]

2014 թվականի Ուկրաինայի նախագահական ընտրությունների ժամանակ տեղի ունեցավ այժմ արդեն աղմկահարույց մի դեպք: Ռուս հաքերները ներթափանցել են Կենտրոնական ընտրական հանձնաժողովի ցանց և տեղադրել կեղծ արդյունքներ՝ ցույց տալով ծայրահեղ ազգայնականների հաղթանակը: Չնայած ուկրաինական կիբեռանվտանգության ստորաբաժանումները ժամանակին չեզոքացրին վնասակար ծրագիրը, ռուսական պետական լրատվամիջոցները շարունակեցին հեռարձակել կեղծ հաղթանակը՝ հանրությանը խաբելու համար:[146] Այս միջադեպը ընդգծում է, թե ինչպես նույնիսկ կանխված կիբեռհարձակումը կարող է օգտագործվել տեղեկատվական պատերազմում՝ օրինական արդյունքները կասկածի տակ դնելու համար:

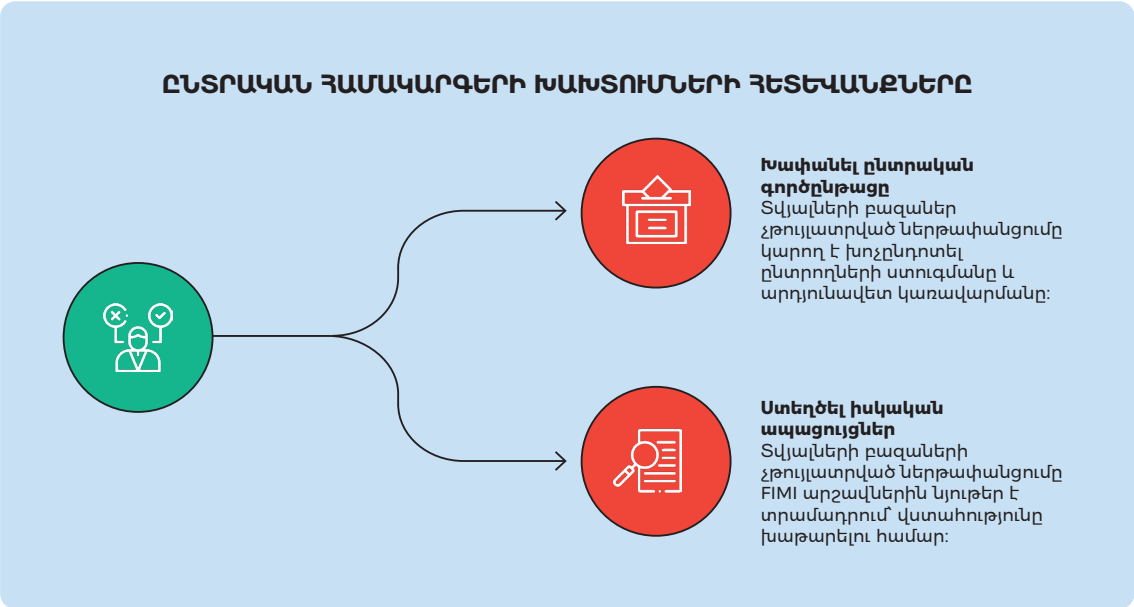
Հակամարտության գոտիներում կամ բարձր լարվածության տարածաշրջաններում ենթակառուցվածքներին ուղղված կիբեռսպառնալիքները հաճախ ուղեկցվում են

ֆիզիկական և FIMI գործողություններով: Ուկրաինայի ընտրական ենթակառուցվածքը 2014 թվականից ի վեր բազմիցս ենթարկվել է հարձակումների՝ որպես Ռուսաստանի հիբրիդային պատերազմի մաս: 2014 թվականի դեպքից հետո Ուկրաինայի ընտրությունների տեղեկատվական համակարգերը մշտական ստուգումների թիրախ են եղել. պաշտոնյաները հայտնել են 2019 թվականի ընտրություններին ընդառաջ ընտրական հանձնաժողովների աշխատակիցների վրա ֆիշինգի և վնասակար ծրագրերի հարձակումների ալիքների մասին:[147] 2022 թվականից ի վեր շարունակվող պատերազմն ավելի է սրել մտահոգությունները. Ուկրաինայում ցանկացած ապագա ընտրություն, որը ներկայումս կասեցված է ռազմական դրության պատճառով, հավանաբար կանցկացվի կիբեռսպառնալիքների չափազանց բարձր մակարդակի պայմաններում, այդ թվում՝ քվեարկության ընթացքում էլեկտրաէներգետիկ ցանցերի կամ կապի ցանցերի վրա խաթարող հարձակումների հնարավորության պայմաններում:[148]

Ուկրաինայի և նմանատիպ առաջնագծի պետությունների դասն այն է, որ ընտրական ենթակառուցվածքների պաշտպանությունը ոչ միայն տեխնիկական ջանք է, այլև ազգային անվտանգության հրամայական, որը պահանջում է դիմակայունության պլանավորում ամենավատ սցենարների, այդ թվում՝ պատերազմական պայմանների համար:

> *«Ընտրական համակարգերը ներկայացնում են գործառնական և տեղեկատվական սպառնալիքների մի ամբողջություն: Հակառակորդը կարիք չունի մեկ ձայն անգամ փոխելու՝ ռազմավարական հաղթանակի հասնելու համար:»*

Ընտրական համակարգերը ներկայացնում են գործառնական և տեղեկատվական սպառնալիքների մի ամբողջություն: Հակառակորդը կարիք չունի մեկ ձայն անգամ փոխելու՝ ռազմավարական հաղթանակի հասնելու համար: Հաջողությամբ ներխուժելով ընտրողների տվյալների բազա՝ հարձակվողը կարող է միաժամանակ երկու նպատակի հասնել: Նախ, նրանք խաթարում են ընտրական գործընթացը՝ խոչընդոտելով պաշտոնյաների կարողությունը ստուգելու ընտրողներին և արդյունավետ կերպով կառավարելու գործընթացը: Երկրորդ, և ավելի կարևորը, դրանք ստեղծում են հզոր, իսկական «ապացույցներ», որոնք կարող են օգտագործվել ընտրությունների լեգիտիմության նկատմամբ վստահությունը խաթարելուն ուղղված FIMI արշավները խթանելու համար: Սա այս տվյալների բազաները դարձնում է, թերևս, հիբրիդային սպառնալիքի գործոնի համար ամենաարժեքավոր թիրախը, քանի որ դրանց վարկաբեկումը միաժամանակ ծառայում է մի քանի ռազմավարական նպատակների:



Ընտրողների գրանցման տվյալների բազաների մշտական խոցելիությունը

Ընտրողների գրանցման համակարգերը կիբեռհարձակումների և խախտումների հիմնական թիրախն են: Փրկագնային ծրագրերով հարձակումները անմիջականորեն ազդել են ընտրական վարչարարության վրա՝ թիրախավորելով այս համակարգերը: 2024 թվականին Միացյալ Նահանգներում տեղի ունեցած միջադեպը ստիպեց շրջաններից մեկին խզել իր կապը նահանգի ընտրողների գրանցման համակարգի հետ՝ որպես նախազգուշական միջոց:[149] Նմանապես, 2024 թվականի վերջին, Կենտուկիի Ջեֆերսոն շրջանի քարտուղարի գրասենյակի վրա Ռուսաստանի հետ կապված փրկագին պահանջող ծրագրային հարձակումը, չնայած չվտանգեց քվեարկության համակարգը, խաթարեց գործունեությունը և ընդգծեց փոխկապակցված կառավարական համակարգերի խոցելիությունը:[150]

Ընտրողների գրանցման տվյալների բազաները որոշում են, թե ով կարող է քվեարկել և որտեղ: Եթե հարձակվողները դրանք անհասանելի դարձնեն՝ փրկագին պահանջող ծրագրերի կամ ծառայությունից հրաժարվելու միջոցով, կամ գաղտնի կերպով փոփոխեն գրառումները, ինչպիսիք են հասցեները կամ անձը հաստատող փաստաթղթերը, հավանական հետևանքները կներառեն ավելի երկար հերթեր, նախնական քվեաթերթիկների օգտագործման աճ, ընտրողների ժամանում սխալ ընտրատեղամաս և ընտրելու իրավունքի վերաբերյալ վեճեր, նույնիսկ եթե ձայների հաշվարկն ինքնին չի տուժում:

Հարձակվողների դրդապատճառները եռակի են. հասանելիություն, որը նշանակում է կիբեռխաթարումներ, որոնք արգելափակում են ընտրողների գրանցումը կամ ընդհատում են էլեկտրոնային ընտրացուցակների համաժամեցումը (ընտրատեղամասերի և կենտրոնական համակարգերի միջև ընտրողների ցուցակների իրական ժամանակի թարմացումը), ամբողջականություն, որը ներառում է գրառումների խմբագրում կամ ջնջում՝ շփոթություն կամ քաղաքացիների ընտրական իրավունքի ընտրովի զրկումներ ստեղծելու նպատակով, և գաղտնիություն՝ անձնական տվյալների գողության միջոցով՝ վախեցնելու կամ թիրախային ֆիշինգի համար: Գողացված տվյալները կարող են նաև օգտագործվել այլ ընտրական համակարգերում ներդրվելու համար:

Ընտրողների տվյալների գողությունը լայն տարածում ունեցող խնդիր է: ԱՄՆ նահանգներից արտահոսած տվյալները կազմում են մութ համացանցում շրջանառվող բոլոր ընտրողների տվյալների մոտ 78 տոկոսը, ընդ որում՝ խախտումներ են գրանցվել առնվազն 23 նահանգներում: Այս բացահայտված տեղեկատվությունը այնուհետև օգտագործվում է նպատակային ապատեղեկատվության, ընտրողների ճնշման մարտավարության և ինքնության մանիպուլյացիայի համար՝ ընտրատեղամասերի վերաբերյալ մոլորեցնող հաղորդագրություններ ուղարկելու կամ նույնիսկ կեղծ քվեարկության փորձ կատարելու հնարավորությամբ:[151]

Կրկնակի սպառնալիք՝ փրկագին պահանջող ծրագրեր և DDoS հարձակումներ

DDoS հարձակումները շարունակում են մնալ ընտրություններին վերաբերող կայքերի, այդ թվում՝ ընտրողների տեղեկատվական պորտալների և արդյունքների մասին հաղորդող կայքերի մուտքը խափանելու տարածված մարտավարություն:[152] 2024 թվականի ԱՄՆ ընտրությունների ցիկլում նկատվեց նման հարձակումների զգալի աճ, որոնք թիրախավորում էին քարոզարշավի կայքերը, կուսակցությունները և շրջանային մակարդակի ենթակառուցվածքները: Կիբեռանվտանգության Cloudflare ընկերությունը հայտնել է, որ միայն 2024 թվականի նոյեմբերի առաջին վեց օրերին ԱՄՆ ընտրություններին առնչվող օբյեկտներին ուղղված ավելի քան 6 միլիարդ չարամիտ հարցումներ են արգելափակվել, ընդ որում՝ որոշ հարձակումների արդյունքում դրանց թիվը հասել է վայրկյանում 700,000-ի:[153] Նմանատիպ քաղաքական դրդապատճառներով DDoS արշավներ նկատվել են 2024 թվականի Եվրախորհրդարանի ընտրությունների ժամանակ, երբ հոլանդական կուսակցությունների կայքերը անջատվել են:[154]

Այս հարձակումների ռազմավարական նպատակը հաճախ գերազանցում է տեխնիկական խափանումները: Ինչպես հրապարակավ նշել են CISA-ն և ԱՄՆ Հետաքննությունների

դաշնային բյուրոն, չնայած DDoS հարձակումները քիչ հավանական է, որ կանխեն քվեարկելու իրավունք ունեցող որևէ ընտրողի մասնակցությունը, դրանք կարող են արդյունավետորեն խոչընդոտել հանրային հասանելիությունը պաշտոնական տեղեկատվությանը և ստեղծել քաոսի և անգործունակության զգացողություն:[155] Այս ընկալումը հետագայում կարող է օգտագործվել ապատեղեկատվական արշավների կողմից, որոնք կարող են խորացնել միջադեպը՝ խաթարելով հանրության վստահությունը ընտրությունների ընդհանուր ամբողջականության և, ընդլայնմամբ, ժողովրդավարական սկզբունքների, արժեքների և գործընթացների նկատմամբ:[156]

Նմանապես, փրկագին պահանջող ծրագրային հարձակումները տեղական ինքնակառավարման մարմինների վրա, նույնիսկ եթե ուղղակիորեն չեն թիրախավորում ընտրական գրասենյակները, կարող են զգալի կողմնակի վնաս պատճառել: 2024 թվականի երկրորդ եռամսյակում գրանցվել է նահանգային, տարածաշրջանային, ցեղային և տարածքային կառավարություններին թիրախավորող փրկագին պահանջող ծրագրերի միջադեպերի աճ: Այս հարձակումները կարող են խաթարել ընտրական պաշտոնյաների աշխատանքը, ովքեր ապավինում են շրջանի ընդհանուր տեղեկատվական ենթակառուցվածքին:[157] Միջադեպերը պարզապես տեխնիկական խնդիրներ չեն, դրանք տեղեկատվական ազդեցության գործողությունների գործիքներ են: Նրանց հիմնական թիրախը սերվերը չէ, այլ՝ հանրային ընկալումը: Հակառակորդի հաջողությունը չափվում է ոչ թե սերվերների խափանումներով, այլ գրված լրատվական հոդվածներով և սոցիալական ցանցերում «հաքերային ընտրությունների» մասին պատմություններ տարածող գրառումներով: Սա նման միջադեպին ռազմավարական հաղորդակցության արձագանքը դարձնում է նույնքան կարևոր, որքան տեխնիկական արձագանքը:

Ընտրական տեխնոլոգիաների մատակարարման շղթայի խաթարումը

Ընտրական տեխնոլոգիաների անվտանգությունը մեծապես կախված է բարդ ծրագրային ապահովման մատակարարման շղթայից, որը դարձել է բարդ հակառակորդների հիմնական թիրախը:[158] Այս համատեքստում ծրագրային ապահովման մատակարարման շղթայի վրա հարձակումների հաճախականությունը շարունակում է աճել, 2024-ի վերջից մինչև 2025-ի կեսերը միջադեպերի թիվն աճել է 25 տոկոսով:[159]

Այս սպառնալիքների բնույթը զգալիորեն փոխվել է: Ծրագրային թարմացումների մեջ չարամիտ կոդի դասական ներդրումից կամ «փաթեթների խեղաթյուրումից» բացի, 2025 թվականի զեկույցը մատնանշել է ավելի խորամանկ միտում՝ ազատ արձակված ծրագրավորողների գաղտնիքների 12 տոկոս աճ. ծառայությունների միջև նույնականացման համար օգտագործվող կոշտ կոդավորված գաղտնաբառերը, թոքենները և API բանալիները, որոնք հայտնաբերվել են առևտրային ապրանքների մեջ ներկառուցված:[160] Ամփոփելով՝ այս օրինաչափությունները ցույց են տալիս, որ հակառակորդները թիրախավորում են ծրագրային ապահովման մշակման ամբողջ կենսացիկլը, այլ ոչ թե միայն վերջնական արտադրանքը: Միևնույն ժամանակ, բաց կոդով ծրագրային ապահովման լայնորեն օգտագործումը և արհեստական բանականության մշակման գործիքների աճը ընդլայնել են բարդ հարձակման մակերեսները, որոնք կարող են շահագործվել:[161]

Խոշոր ծրագրային ապահովման և ծառայությունների մատակարարների մոտ տեղի ունեցած աղմկահարույց խախտումները ցույց են տալիս մեկ մատակարարման շղթայի խախտման կասկադային երրորդ կողմի ազդեցությունը, որը ազդում է հետագա օղակներում գտնվող հազարավոր հաճախորդների վրա:[162] Դրանք ծառայում են որպես նախազգուշացում ընտրական տեխնոլոգիաների ոլորտի համար, որը հույսը դնում է նմանատիպ երրորդ կողմի բաղադրիչների և ծառայությունների վրա: Ընտրական համակարգերի համար սա նշանակում է, որ վտանգները տարածվում են համատեղ մատակարարների և բաղադրիչների միջոցով: Սպառնալիքը պարզապես «արտադրանքի վարակումից» տեղափոխվել է գործընթացի համակարգված խաթարման: Ծրագրավորողի մուտքի տվյալները գողանալով կամ չպաշտպանված կառուցվածքը շահագործելով՝ հակառակորդը կարող է մշտական մուտք և բազմաթիվ ուղիներ ստանալ ապագայում շահագործման համար:

«Սպառնալիքը պարզապես «արտադրանքի վարակումից» փեղափոխվել է գործընթացի համակարգված խաթարման։»

Այլ կերպ ասած, սա ավելի ռազմավարական, երկարաժամկետ փոխզիջում է, որը զգալի բեռ է դնում ընտրական պաշտոնյաների վրա գնումների գործընթացի ընթացքում: Նրանք այլևս չեն կարող վստահել վաճառողի հավաստագրմանը. նրանք նաև պետք է մանրակրկիտ ուսումնասիրեն վաճառողի նախագծային անվտանգ մշակման գործելակերպը: Հետևաբար, կրիտիկական խոցելիությունը կարող է գտնվել ոչ թե ընտրություններին հատուկ կոդում, այլ այն երրորդ կողմի գրադարանում, որից այն կախված է, ինչը հայտնաբերումն ու շտկումը դարձնում է շատ ավելի դժվար:

4.3. ԿԻԲԵՌՀԱՐՁԱԿՈՒՄՆԵՐ, ՈՐՈՆՔ ԹԻՐԱԽԱՎՈՐՈՒՄ ԵՆ ՔԱՐՈԶԱՐՇԱՎՆԵՐԸ, ԿՈՒՍԱԿՑՈՒԹՅՈՒՆՆԵՐԸ ԵՎ ԸՆՏՐԱԿԱՆ ՊԱՇՏՈՆՅԱՆԵՐԻՆ

Քաղաքական արշավները, կուսակցությունները և պաշտոնյաները ընտրություններին ազդելու նպատակով կիբեռհարձակումների հիմնական թիրախներն են:[163] Ամենաազդեցիկ մարտավարությունը «հաքերային հարձակում և արտահոսք» գործողությունն է, որի ընթացքում գողացված նյութերը, ինչպիսիք են էլեկտրոնային նամակները և փաստաթղթերը, ռազմավարական առումով հրապարակվում են առցանց՝ ապատեղեկատվություն տարածելու և առավելագույն քաղաքական վնաս պատճառելու համար:[164] Այս գործնական ուղեցույցը բազմիցս օգտագործվել է՝ սկսած 2016 թվականի ԱՄՆ-ի և 2017 թվականի Ֆրանսիայի ընտրություններում Ռուսաստանի գործողություններից մինչև 2024 թվականին Իրանի հետ կապված հաքերների կողմից ԱՄՆ նախագահական քարոզարշավի տվյալների խախտումը: Այս հարձակումները հաճախ սկսվում են թիրախային ֆիշինգի միջոցով, որը ներառում է բարձր մակարդակի հարմարեցված էլեկտրոնային նամակներ՝ մարդկանց խաբելու և իրենց մուտքային տվյալները բացահայտելու համար:[165]

Աճող սպառնալիքներից մեկը արհեստական բանականության միջոցով ձայնի կլոնավորումն է, որը հայտնի է նաև որպես «վիշինգ», որի դեպքում հակառակորդը օգտագործում է արհեստական բանականությունը՝ հեռախոսով վստահելի անձի ձայնը կրկնօրինակելու համար: CISA-ն զգուշացնում է, որ այս մարտավարությունը կարող է օգտագործվել բարձրաստիճան ընտրական պաշտոնյաներին կրկնօրինակելու համար:[166]

Ընտրական պաշտոնյաները նաև բախվում են սպառնալիքների մի շարք, այդ թվում՝ ֆիշինգ և դոքսինգ (անձնական տեղեկատվության չարամիտ հրապարակում), թե՛ օտարերկրյա, թե՛ ներքին դերակատարների կողմից, որոնք փորձում են վախեցնել կամ գողանալ նրանց մուտքային տվյալները:[167] Այս գործիքները անհամաչափորեն օգտագործվել են քաղաքականության և լրագրության ոլորտում կանանց դեմ՝ ոտնձգությունների և ոչ համաձայնեցված խորը կեղծ պոռնոգրաֆիայի ստեղծման միջոցով:[168]

Այս զարգացումը նշանակում է, որ քարոզարշավները, կուսակցությունները և պաշտոնյաները պետք է ենթադրեն մշտական թիրախավորում ողջ ընտրական ցիկլի ընթացքում և նախապես պատրաստվեն մուտքային տվյալների գողության և հաքերային գործողությունների ու արտահոսքի փորձերին: Երբ հետախուզական տվյալները մատնանշում են անխուսափելի արտահոսք, չափված կանխարգելիչ վերագրումը կարող է մեղմել ազդեցությունը: Քանի որ արհեստական բանականությունը բարձրացնում է խայծի որակը և հնարավորություն է տալիս ձայնային կեղծման, պետական մարմինները պետք է արգելեն միայն ձայնային հաստատումները և պահանջեն հետադարձ զանգի կամ երկրորդ ալիքի ստուգում: Անհրաժեշտ է նաև պաշտպանել մարդկանց և համակարգերը՝ գենդերային խտրականության ենթարկվող դիփֆեյքերի բախվող կանանց համար իրավական և աջակցության ուղիներ ապահովելու և պաշտոնյաներին դոքսինգից և ոտնձգություններից պաշտպանելու համար:[169]

4.4. Ի՞ՆՉ ԿԱՐԵԼԻ Է ԱՆԵԼ: ԸՆՏՐԱԿԱՆ ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԴԻՄԱԿԱՅՈՒՆՈՒԹՅԱՆ ԼԱՎԱԳՈՒՅՆ ՓՈՐՁԸ

Ժամանակակից կիբեռ և տեղեկատվական սպառնալիքների դեմ արդյունավետ պաշտպանությունը պահանջում է շարունակական, հարմարվողական և համագործակցային մոտեցում:[170] Լայն կոնսենսուս է ձևավորվել լավագույն փորձի մի ամբողջության շուրջ, որը կազմում է ընտրական կիբեռանվտանգության դիմակայունության միջուկը:[171] Միասին վերցրած, այս շերտերը տեխնիկական դիմակայունությունը վերածում են ընտրական լեգիտիմության: Կառավարման և նախագծման միջոցով անվտանգության սկզբունքները նվազեցնում են սխալների մակարդակը և վերացնում ձախողման միակ կետը: Նախաձեռնողական գործողությունները և փորձնական արձագանքը նվազագույնի են հասցնում հարձակվողի վրա ազդեցության ժամանակը և խափանումների տեսանելիությունը՝ փակելով տեղեկատվական վակուումները: Իսկ տարեկան գործընկերությունները հնարավորություն են տալիս ապահովել հավաստի, բազմագործակալական հաղորդակցություն և անկախ ստուգում:

Արդյունքը ծառայության շարունակականությունն է՝ ապահովելով, որ մարդիկ կարողանան քվեարկել՝ զուգորդված ազնվության ապացույցների հետ, ինչը նշանակում է, որ արդյունքները ենթակա են աուդիտի, և վստահելի բացատրության հետ, որը ապահովում է, որ հանրությունը հասկանա, թե ինչ է տեղի ունեցել և ինչու: Այս երեք պայմանները պահպանում են ընտրությունների ինչպես ենթադրյալ, այնպես էլ իրական լեգիտիմությունը:

Հիմնարար կառավարում և տեխնոլոգիա

Դիմակայունությունը սկսվում է ամբողջ ընտրական էկոհամակարգի համապարփակ ռիսկերի գնահատմամբ՝ սկսած ընտրողների գրանցումից մինչև արդյունքների մասին հաղորդումը:[172] Այս հիմքի վրա հիմնվելով՝ ընտրական մարմինները պետք է ընդունեն նախագծմամբ ապահով տեխնոլոգիաներ՝ պահանջելով մատակարարներից անվտանգությունը ներկառուցել ծրագրային ապահովման մշակման ողջ կյանքի ցիկլի ընթացքում:[173] Գործնականում սա ավելի ու ավելի է ենթադրում «Զրոյական վստահություն» կառուցվածքի ներդրում, որը վերացնում է անուղղակի վստահությունը և անընդհատ

ստուգում է կարևոր համակարգերին միացված յուրաքանչյուր օգտատիրոջ, սարքի և աշխատանքային բեռնվածություն:[174] Այս բազային ընտրությունները նվազեցնում են ձախողման միակ կետը և հետագա վերահսկողությունն ավելի արդյունավետ են դարձնում:

Նախաձեռնողական գործողություններ և արձագանք

Պաշտպանական կեցվածքը պետք է լինի նախաձեռնողական: Սա նշանակում է համակարգերի անընդհատ ամրապնդում տեխնիկական վերահսկողության միջոցով, ինչպիսիք են բազմագործոն նույնականացումը և ցանցի սեգմենտացումը, սպառնալիքների մոնիթորինգը՝ ներխուժման հայտնաբերման միջոցով, և նախապես տեղադրված վնասակար ծրագրերի ակտիվ որոնումը ընտրություններից շատ առաջ:[175] Նույնքան կարևոր է նաև միջադեպերին արձագանքման լավ մշակված ծրագրեր ունենալը, որոնք համատեղում են տեխնիկական զսպումը ռազմավարական հաղորդակցության հետ՝ կանխելով գործառնական խնդիրների վերաճումը լեգիտիմության ճգնաժամի:[176] Այս օպերացիոն կարգապահությունը տեխնիկական դիմակայունությունը վերածում է հանրային վստահության:

Կայուն համագործակցություններ

Ի վերջո, մեկուսացման մեջ արդյունավետ պաշտպանություն անհնար է: Դիմակայունությունը կախված է ամբողջ տարվա գործընկերություններից և ընտրությունների ոլորտում համագործակցության ամուր ցանցերի ստեղծումից: Այս կառույցները պաշտոնականացնում են ընտրությունների կառավարման մարմինների (ԸԿՄ), կիբեռանվտանգության գործակալությունների, հետախուզական ծառայությունների և իրավապահ մարմինների միջև համագործակցությունը՝ ստեղծելով ի հայտ եկող սպառնալիքներին արագ և համակարգված արձագանքելու համար անհրաժեշտ համատեղ իրազեկվածությունը:[177] Կապելով կառավարումը, օպերացիոն գործելակերպը և համագործակցությունները՝ իշխանությունները կարող են ավելի վաղ հայտնաբերել, ավելի արագ արձագանքել և ավելի հավաստիորեն հաղորդակցվել՝ այդպիսով ամրապնդելով ընտրությունների ինչպես ենթադրյալ, այնպես էլ իրական լեգիտիմությունը:

05 Ընտրությունների հիբրիդ սպառնալիքներին հակազդելը. Ընտրական համագործակցության ցանցերի ստեղծման անհրաժեշտությունը

Հիբրիդային սպառնալիքների բազմադոմեյնային և բազմաշահագրգիռ բնույթը ավանդական, մեկուսացված անվտանգության միջոցառումները դարձնում է անբավարար: Հակառակորդները դիտավորյալ շահագործում են գործակալությունների պարտականությունների համընկնումները, օրինակ՝ ընտրությունների ժամանակ, միաժամանակ հարձակվելով կիբեռենթակառուցվածքների, տեղեկատվական միջավայրի և ֆիզիկական անվտանգության վրա: Ընտրությունների կազմակերպման մարմինը (EMB) կարող է պատրաստ լինել լոգիստիկ մարտահրավերներին, կիբեռանվտանգության գործակալությունը՝ ցանցի ներխուժումներին, իսկ իրավապահ մարմինները՝ ֆիզիկական անվտանգության սպառնալիքներին, բայց դրանցից և ոչ մեկն առանձին հագեցած չէ երեքն էլ միավորող համաժամեցված հարձակմանը դիմակայելու համար:[178] Չարամիտ գործողները հասկանում են այս ինստիտուցիոնալ բաժանումները և իրենց գործողությունները նախագծում են դրանք շահագործելու համար՝ ստեղծելով ռազմավարական մարտահրավեր, որը կարող է հաղթահարվել միայն հավասարապես ինտեգրված և ցանցային պաշտպանության միջոցով:[179] Հետևաբար, արդյունավետ պաշտպանությունը պահանջում է հիմնարար անցում դեպի ամուր, մշտական ընտրական համագործակցության ցանցերի ստեղծում՝ թե՛ ազգային, թե՛ միջազգային մակարդակներում:[180]

Այս ցանցերը կարևոր են համագործակցության ինստիտուցիոնալացման համար՝ անցնելով արտակարգ ճգնաժամերի կառավարումից այն կողմ՝ նախաձեռնողական, դիմացկուն պաշտպանական դիրքորոշում կառուցելու համար: Այս ցանցերի հիմնական նպատակն է մշակել ընդհանուր գործառնական պատկեր բոլոր հիմնական դերակատարների միջև՝ նպաստելով ի հայտ եկող սպառնալիքների արագ, համակարգված հայտնաբերմանը և դրանց արձագանքին: Հիբրիդային սպառնալիքներին հակազդելու եվրոպական գերազանցության կենտրոնի կողմից մշակված ընտրություններին ուղղված հիբրիդային սպառնալիքներին հակազդելու համապարփակ շրջանակը սահմանում է այն հիմնական գործառույթները, որոնց վրա պետք է կենտրոնանան այդ ցանցերը, ներառյալ օրենսդրության թարմացումը, խոցելիության գնահատման անցկացումը, դիմակայունության խթանումը, հաղորդակցության բարելավումը, համատեղ վարժանքների անցկացումը և հայտնաբերման ու արձագանքման կարողությունների ամրապնդումը:[181]

Այս նախաձեռնողական ցանցային մոտեցումը համապատասխանում է եվրոպական մակարդակի պաշտոնական ուղեցույցներին: Եվրոպական հանձնաժողովը հստակորեն խորհուրդ է տվել անդամ պետություններին ստեղծել ազգային ընտրական համագործակցության ցանցեր՝ դրանք ճանաչելով որպես կարևոր հարթակներ ընտրական իշխանությունների համար՝ այլ կարևոր անվտանգության մարմինների հետ համագործակցելու նպատակով: Հանձնաժողովը նշում է, որ նման համագործակցությունը կարևոր է սպառնալիքների արագ հայտնաբերման և կանոնների արդյունավետ կիրառման համար:[182]

Վերջերս ընտրությունների պաշտպանության ջանքերից ստացված կարևոր դասն այն է, որ ճգնաժամի ժամանակ համագործակցությունը չի կարող «տեղում հորինվել»: Հարաբերությունները, վստահությունը և տեղեկատվության փոխանակման արձանագրությունները պետք է հաստատվեն և փորձարկվեն նախօրոք, քանի որ ճնշման տակ կազմավորված իմպրովիզ միջոցառումները հաճախ անարդյունավետ են: Հետևաբար, մշտական, պաշտոնական համագործակցության ցանցերի ինստիտուցիոնալացումը ոչ միայն լավագույն փորձ է, այլև հիմնարար նախապայման՝ ժամանակակից հիբրիդային սպառնալիքների քրոնիկ ճնշմանը դիմակայելու համար անհրաժեշտ դիմակայունությունը ձևավորելու համար:[183]

5.1. ԱԶԳԱՅԻՆ ՀԱՄԱԳՈՐԾԱԿՑՈՒԹՅԱՆ ԿԱՌՈՒՑՎԱԾՔՆԵՐ

Թեև համագործակցային պաշտպանության սկզբունքը լայնորեն ընդունված է, ընտրական համագործակցության ցանցի համար «բոլորին համապատասխանող» մոդել գոյություն չունի: Ազգային կառուցվածքները ձևավորվում են երկրի յուրահատուկ կառավարման և իր առջև ծառացած սպառնալիքների վերաբերյալ նրա ընկալումների հիման վրա: Ստորև բերված օրինակները ամփոփում են յուրաքանչյուր մոդելի հիմնական մեխանիզմը և շրջանակը:

- Շվեդիայի ապակենտրոնացված կառավարումը և կոնսենսուսի վրա հիմնված մշակույթը ստեղծում են համագործակցության մոդելի վրա հիմնված բազմամակարդակ ցանց: Ազգային մակարդակում Շվեդիայի ընտրական մարմինը նախագահում է ազգային ընտրական համագործակցության ցանց, որը լրացվում է տարածաշրջանային և տեղական ցանցերով:[184] Գործնական առանձնահատկություններից են մշտական տեղեկատվության փոխանակման խմբերը, համատեղ պարբերական վարժանքները և դերերի հստակ տարանջատումը ազգային մակարդակում տրամադրվող ուղեցույցների և համայնքային մակարդակում իրականացվող գործնական քայլերի միջև:

- Միացյալ Նահանգների խիստ ֆեդերալացված կառուցվածքն անհրաժեշտ է դարձնում ապակենտրոնացված մոդել, որի դեպքում դաշնային գործակալությունները համակարգվում են 50 անկախ կառավարվող նահանգային ընտրական համակարգերի հետ: Համակարգումն իրականացվում է կամավոր շրջանակների միջոցով, ինչպիսիք են Ընտրական ենթակառուցվածքների տեղեկատվության փոխանակման և վերլուծության կենտրոնը, համատեղ ձեռնարկները և միջադեպերին արձագանքման աջակցությունը, այլ ոչ թե կենտրոնացված ուղղորդումը:[185]

- Ֆրանսիայի վիճակագրական ավանդույթը հանգեցրել է հատուկ պետական մարմնի ստեղծմանը, որն իրավասու է հրապարակայնորեն բացահայտել արտաքին միջամտությունը: Այս մարմինը՝ Viginum-ը (Service de vigilance et de Defense contre les ingérences numériques étrangères), մարմնավորում է կենտրոնացված մոդել, որն առաջնահերթություն է տալիս հետաքննական լիազորություններին, արագ հանրային զգուշացումներին և պետական ողջ համակարգի մակարդակով հանձնարարականների փոխանցմանը օպերացիոն ստորաբաժանումներին:[186]

- Կանադան մշակել է հետախուզության վրա հիմնված մոդել, որը շատ լավ մեկուսացված է անմիջական քաղաքական ոլորտից:[187] Այս մոդելը կենտրոնանում է ընտրություններին սպառնացող անվտանգության և հետախուզության հարցերով աշխատանքային խմբի վրա, որը իրականացնում է սպառնալիքների ինտեգրված գնահատում, և կրիտիկական ընտրական միջադեպերի հանրային արձանագրության հանձնաժողովի վրա, որը կառավարում է շեմի վրա հիմնված հանրային հաղորդակցությունը: Կանադայի ընտրությունների մարմինը ո՛չ աշխատանքային խմբի, ո՛չ էլ արձանագրությունների հանձնաժողովի անդամ չէ: Այն մնում է անկախ, բայց համակարգում է իր գործունեությունը անվտանգության մարմինների հետ և ստանում է ճեպազրույցներ:[188]

Այս օրինակները ցույց են տալիս, որ չնայած համագործակցության հիմնական գործառույթները համընդհանուր են, ինստիտուցիոնալ ձևը պետք է հարմարեցվի ազգային համատեքստին: Իրենց կոնկրետ կառուցվածքներից զատ, արդյունավետ ընտրական համագործակցության ցանցերը կիսում են մի շարք հիմնական օպերացիոն գործառույթներ և լավագույն փորձ, որոնք էական են հաջողության համար: Այս գործելակերպը երկրի պաշտպանական կեցվածքը ռեակտիվ, իրադարձություններով պայմանավորվածից փոխում է դեպի նախաձեռնողական, շարունակական: Տարբեր ազգային մոդելների վերլուծությունը ցույց է տալիս մի ընդհանուր գործողությունների փաթեթ այն. մասին, թե ինչ պետք է անեն այս ցանցերը արդյունավետ լինելու համար:

Ընդհանուր իրավիճակային պատկերի ստեղծում. Միաձուլման բջիջի (միավորված վերլուծական խումբ) հայեցակարգը

Արդյունավետ համագործակցության հիմնարար գործելակերպը «միաձուլման բջիջի» ստեղծումն է: Այս հայեցակարգը ենթադրում է բոլոր մասնակից գործակալությունների վերլուծաբանների և կապի պատասխանատուների համատեղ տեղակայում՝ անձամբ կամ վիրտուալ եղանակով՝ իրական ժամանակում տեղեկատվության փոխանակում ապահովելու և սպառնալիքների միջավայրի վերաբերյալ ընդհանուր ըմբռնում խթանելու համար:[189] Տեղեկատվության մենաշնորհները վերացնելով՝ տարբեր մասնագետներից կազմված միաձուլման խմբերը՝ կիբեռ պատասխանողներից մինչև հետախուզական վերլուծաբաններ և ռազմավարական հաղորդակիցներ. կարող են միավորել բազմաթիվ սպառնալիքների հոսքերը մեկ, համահունչ «ընդհանուր իրավիճակային պատկերի» մեջ:

Վերլուծական ինտեգրացիան ինստիտուցիոնալ ինքնավարության հետ հավասարակշռելու համար միավորված բջիջները պետք է գործեն «միասին վերլուծեք, գործեք մանդատի սահմաններում» սկզբունքով. վերլուծությունը կլինի համատեղ, մինչդեռ գործառնական որոշումներն ու լիազորությունները կմնան յուրաքանչյուր հաստատության ներսում: Այս համատեղ գիտակցումը համակարգված արձագանքի հիմքն է և կարող է նախագծվել՝ հարգելով EMB-ի գործառնական անկախությունը:[190]

Գործնականում հավասարակշռությունն պահպանվում է նպատակով սահմանված տվյալների փոխանակման և դերերի վրա հիմնված հասանելիության, պաշտոնական փոխըմբռնման հուշագրերի, վերլուծության և օպերացիոն գործունեության միջև խիստ տարանջատման, ինչպես նաև աուդիտի ենթակա փոխանակման գրանցամատյանների միջոցով: Լուծումը կայանում է ձևավորման, այլ ոչ թե հեռավորության մեջ. միավորված բջիջները պետք է մնան խիստ վերլուծական՝ սահմանափակված տեղեկատվության փոխանակմամբ, որը գործառնական որոշումները կպահի յուրաքանչյուր հաստատության իրավասության շրջանակներում՝ ապահովելով, որ EMB-ն պահպանի ընտրական գործընթացների նկատմամբ միանձնյա իշխանությունը:

Այս կերպ ներդրվելիս միաձուլման բջիջները տալիս են շոշափելի արդյունքներ, այդ թվում՝ սպառնալիքների ավելի արագ հայտնաբերում և տեսակավորում («հայտնաբերման ժամանակ»), գործակալությունների միջև ջանքերի կրկնօրինակման նվազեցում, ինչպես նաև համատեղ արձագանքներում վստահության և հաղորդագրությունների ներդաշնակության ամրապնդում:

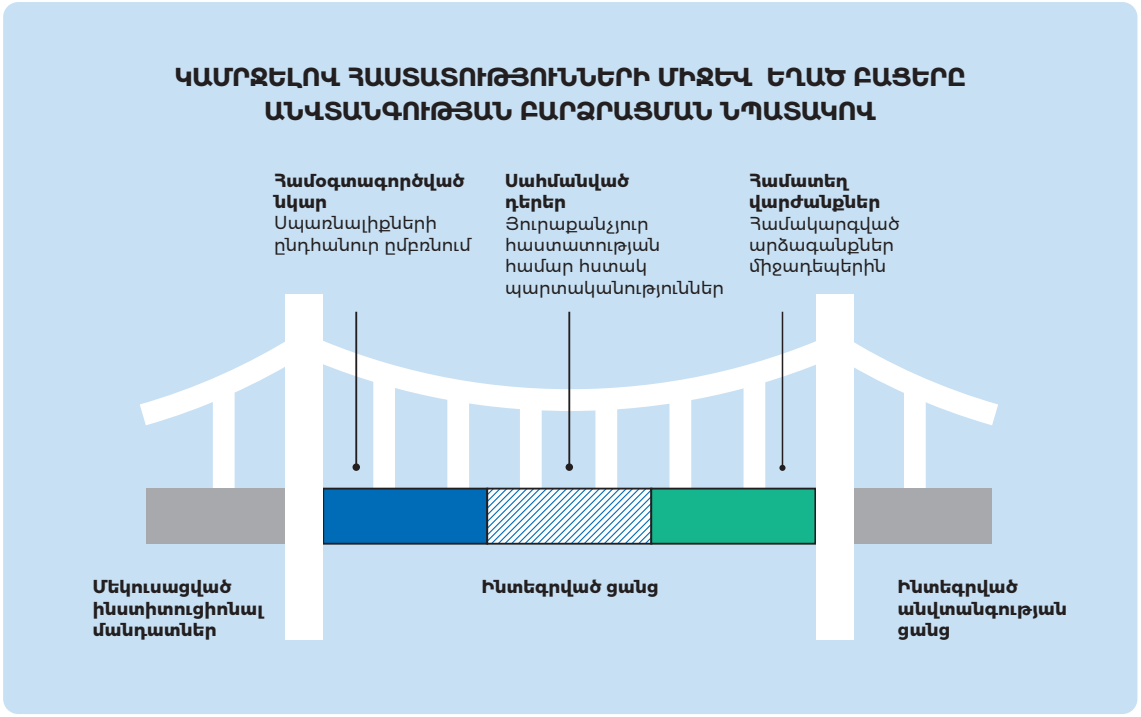
Նախաձեռնողական, շարունակական աշխատանք ընտրական ցիկլերի միջև ընկած ժամանակահատվածում

Արդյունավետ ցանցերը գործում են անընդհատ, այլ ոչ թե միայն քվեարկությանը նախորդող ամիսներին: Հիմնական կանխարգելիչ գործողությունները ներառում են.

- Ռիսկի և խոցելիության համատեղ գնահատումներ. Ընտրական էկոհամակարգի կանոնավոր և համակարգված քարտեզագրում՝ ռիսկերը բացահայտելու և առաջնահերթություն տալու համար, նախքան դրանք կարող են շահագործվել:[191]

- Սցենարային պլանավորում և համատեղ վարժանքներ. Արձագանքման պլանները փորձարկելու, համակարգման բացերը հայտնաբերելու և ինստիտուցիոնալ «մկանային հիշողություն» ձևավորելու համար պարբերաբար անցկացնել սեղանի և գործառնական վարժություններ:[192] ԵՄ-ի կողմից խորհրդարանական ընտրություններից առաջ անցկացվող համատեղ կիբեռանվտանգության վարժանքները դրա հիմնական օրինակն են:[193]

- Տեղեկատվության փոխանակման և արձագանքման պաշտոնականացված ընթացակարգեր. Հստակ, նախապես համաձայնեցված ընթացակարգերի սահմանում, որոնք կարգավորում են սպառնալիքների մասին հաղորդելու, գնահատելու և դրանց նկատմամբ գործողություններ ձեռնարկելու եղանակը: Սա խուսափում է իմպրովիզացիայից ճգնաժամի ժամանակ և օգնում է ապաքաղաքականացնել որոշումների կայացումը:[194]



5.2. ՑԱՆՑԵՐԻ ՑԱՆՑ

Գլոբալացված տեղեկատվական միջավայրում զուտ ազգային պաշտպանությունն անբավարար է և պահանջում է «ցանցերի ցանց», որը միավորում է ազգային մարմինները հզոր միջազգային շրջանակների հետ:

Եվրոպական Միությունն ունի ամենաբարդ տարածաշրջանային էկոհամակարգը: Դրա Ընտրությունների հարցերով Եվրոպական համագործակցության ցանցը (ECNE) ծառայում է որպես կենտրոնական հանգույց ազգային իշխանությունների համար՝ կիբեռրանվտանգությունից մինչև ապատեղեկատվության դեմ պայքար՝ լավագույն փորձի փոխանակման համար:[195] Սա կապված է մասնագիտացված ցանցերի հետ, ինչպիսին է FIMI սպառնալիքների արագ ահազանգման համակարգը, և աջակցվում է Ընտրական

դիմակայունության համատեղ մեխանիզմի կողմից, որը կարող է փորձագիտական խմբեր տեղակայել անդամ պետություններում: Այս ինտեգրված համակարգը համարվում էր կարևորագույն գործոն 2024 թվականի Եվրոպական խորհրդարանի ընտրությունների սահուն անցկացումն ապահովելու համար:[196]

Ավելի լայն համագործակցությունը տարածվում է ՆԱՏՕ-ի միջոցով, որը հիբրիդային սպառնալիքները համարում է անվտանգության հիմնական մարտահրավեր և աշխատում է բարելավել դաշնակիցների միջև հետախուզական տվյալների փոխանակումը, և G7-ի արագ արձագանքման մեխանիզմի (RRM) միջոցով, որը համակարգում է օտար պետությունների կողմից հովանավորվող ապատեղեկատվությանը արձագանքները:[197] Համաշխարհային մակարդակում միջկառավարական կազմակերպությունները, օրինակ՝ Ժողովրդավարության և ընտրությունների աջակցության միջազգային ինստիտուտը (Internatioanl IDEA). կարևոր դեր են խաղում նորմերի ձևավորման և պրակտիկայի համայնքի խթանման գործում՝ «Ընտրական ամբողջականության ապահովման գլոբալ ցանց»-ի նման նախաձեռնությունների միջոցով:[198]

5.3. ԱՐԴՅՈՒՆԱՎԵՏ ՀԱՄԱԳՈՐԾԱԿՑՈՒԹՅԱՆ ՄԱՐՏԱՀՐԱՎԵՐՆԵՐԸ

Չնայած համագործակցային պաշտպանության մեխանիզմների ստեղծման գործում գրանցված զգալի առաջընթացին, դրանց երկարաժամկետ արդյունավետությունն ու կենսունակությունը բախվում են խորը և շարունակական մարտահրավերների: Գործնականում դրանք ներառում են քաղաքական շրջադարձեր և բևեռացում, ֆինանսավորման անկում, իրավական անորոշություն և տվյալների փոխանակման ու համակարգման առօրյա խնդիրներ:

Հիբրիդային սպառնալիքի կայունության հիմնական պարադոքսն այն է, որ հենց այն մեխանիզմները, որոնք ստեղծվել են համակարգված տեղեկատվական, կիբեռ և ֆինանսավորման միջոցով գործադրվող ճնշումներին հակազդելու համար, կարող են իրենք դառնալ թիրախներ՝ խոցելի լինելով FIMI-ով պայմանավորված ապալեգիտիմացման, բևեռացման և իրավական կամ բյուջետային հարձակումների նկատմամբ՝ նույն այն դերակատարների կողմից, որոնց ազդեցությանը դրանք կոչված են դիմակայելու: Պարզ ասած, մեր կառուցած պաշտպանիչ ցանկապատերը կարող են թուլանալ հենց այն ուժերի պատճառով, որոնց զսպման համար են դրանք նախատեսված:

Այս խոչընդոտները, որոնք ընդգրկում են քաղաքական, ֆինանսական և օպերացիոն ոլորտները, սպառնում են քայքայել հենց այն կառույցները, որոնք ստեղծվել են ժողովրդավարական գործընթացները պաշտպանելու համար: Դրանց հասցեագրումը կարևոր է կայուն, այլ ոչ թե դրվագային, դիմակայունության ձևավորման համար:

> *«Կայուն դիմակայունության ուղին պահանջում է ոչ միայն այս ցանցերի ստեղծում, այլև ավելի լայն հասարակական ջանքեր՝ ընտրությունների անվտանգությունը ապաքաղաքականացնելու և այն որպես առանցքային, անսակարկելի ազգային շահ ամրագրելու համար:»*

Հետևաբար, երկարաժամկետ կայունությունը կախված է ինստիտուցիոնալ գործնական մեկուսացումից՝ հստակ մանդատներից, միջկուսակցական աջակցությունից և պաշտպանված բյուջեներից՝ զուգորդված լայնածավալ քաղաքական համախմբման հետ, որը դիմանում է ցանկացած առանձին կառավարության փոփոխությանը: Կայուն դիմակայունության ուղին պահանջում է ոչ միայն այս ցանցերի ստեղծում, այլև ավելի լայն հասարակական ջանքեր՝ ընտրությունների անվտանգությունը ապաքաղաքականացնելու և այն որպես առանցքային, անսակարկելի ազգային շահ ամրագրելու համար: Այն պետք է հիմնված լինի համատեղ սոցիալական համաձայնության և հանրային վստահության վրա և իրականացվի ամբողջ հասարակությանը ներգրավող մոտեցման միջոցով:

06 Եզրակացություններ և առաջարկություններ

2024 թվականից մինչև այսօր ընկած ժամանակահատվածը հստակ ցույց է տալիս, որ հիբրիդային սպառնալիքները ներկայացնում են ամբողջ աշխարհում ընտրական անխաթարության նկատմամբ մշտական, հարմարվողական և ավելի ու ավելի բարդ մարտահրավեր: Ընտրությունները թիրախավորող հիբրիդային հարձակումների վերջին դեպքերի վերլուծությունը ընդգծում է այս սպառնալիքների էվոլյուցիան՝ դրվագային միջամտությունից մինչև հակամարտության քրոնիկ, համակարգային ձև, որն այժմ գործում է որպես համակողմանի արշավ: Այս արշավները համաժամեցնում են FIMI-ն, կիբեռգործողությունները, քաղաքական գործընթացների ապօրինի ֆինանսավորումը, իրավական գործունեությունը և դաշտային/անցանց ճնշումը: Դրանք համակարգվում են պետական, միջնորդ (proxy) և քրեական դերակատարների միջև և ժամանակագրվում են այնպես, որ ընտրական ցիկլի ընթացքում ինստիտուցիոնալ բացերը կարողանան շահագործել:

Վերջին իրադարձությունների վերլուծությունն ընդգծում է մի քանի կարևոր եզրակացություններ.

- **Անցում դեպի քրոնիկ հակամարտություն.** Ընտրական միջամտությունը պարբերաբար տեղի ունեցող միջադեպերից վերածվել է շարունակական տեղեկատվական հակամարտության: Չարամիտ պետական դերակատարները համառորեն աշխատում են խաթարել ժողովրդավարական համակարգերը՝ խաթարելով հանրային վստահությունը, խթանելով բևեռացումը և թուլացնելով ինստիտուտները:[199]

- **Արդյունաբերական մասշտաբի գործողություններ և նոր տեխնոլոգիաներ.** Հակառակորդներն այժմ գործում են արդյունաբերական մասշտաբով՝ օգտագործելով բարդ, կենտրոնացված կառավարվող քարոզչական ցանցերը:[200] Արհեստական բանականության զենքացումը դարձել է ուժի զգալի բազմապատկիչ՝ հնարավորություն տալով ցածր գնով և արագ ստեղծել սինթետիկ լրատվամիջոցներ և գերիրական ապատեղեկատվություն, ինչը զգալիորեն մեծացնում է սպառնալիքների ծավալը և որակը:[201]

- **Սպառնալիքի վեկտորների ինտեգրում.** Հաջողակ հիբրիդային գործողությունները հազվադեպ են հիմնված մեկ մեթոդի վրա: Փոխարենը, նրանք տեղեկատվական մանիպուլյացիաները, քաղաքական ապօրինի ֆինանսավորումը և խաթարող կիբեռհարձակումները ինտեգրում են համախմբված արշավների մեջ: Անօրինական միջոցները, որոնք հաճախ ուղղորդվում են կրիպտոարժույթների և երրորդ կողմերի միջոցով, աջակցում են տեղեկատվական ազդեցության գործունեությանը և ձայների գնմանը: Միևնույն ժամանակ, կիբեռհարձակումները օգտագործվում են «հաքերային և արտահոսքի» գործողությունների համար տվյալներ գողանալու և ընտրական գործընթացները խաթարելու համար՝ սերմանելով շփոթություն և անվստահություն:[202]

- **Հայտնաբերումը, վերագրումը և հաշվետվողականությունը շարունակում են խոչընդոտներ հանդիսանալ.** Պրոքսի սերվերների օգտագործումը, տեղեկատվության լվացումը և տվյալների մասնատված հասանելիությունը խոչընդոտում են ժամանակին և համաչափ արձագանքին: Միևնույն ժամանակ, հարթակների թափանցիկության անհամաչափ մոտեցումները սահմանափակում են արտաքին վերահսկողությունը: Բովանդակության ծագման և հետազոտողների տվյալների հասանելիության բաց ստանդարտների ոլորտում առաջընթացը պետք է զուգակցվի աուդիտի ենթարկվող գովազդային տեխնոլոգիաների վերահսկողության և արդյունավետ պատժամիջոցների ստուգման հետ:[203]

6.1. ԱՌԱՋԱՐԿՈՒԹՅՈՒՆՆԵՐ

Այս արդյունքները ընդգծում են ցանցային պաշտպանություն ձևավորելու և ամրապնդելու անհրաժեշտությունը: Քանի որ հակառակորդները գիտակցաբար շահագործում են հաստատությունների լիազորությունների միջև եղած բացերը, ավանդական մեկուսացված անվտանգության պատասխաններն այլևս բավարար չեն:

Հետևյալ առաջարկությունները ուղղված են ժողովրդավարական գործընթացների պաշտպանության համար պատասխանատու շահագրգիռ կողմերին: Դրանք կազմակերպված են չորս հիմնական գործողությունների շուրջ, որոնք ուղղված են կայուն ազգային և միջազգային դիմակայունության խթանմանը:

1. **Ներքին ինստիտուցիոնալ կարողությունների զարգացում.** Առանձին հաստատությունները պետք է ստանձնեն իրենց սեփական պաշտպանության պատասխանատվությունը՝ հենվելով հստակ մանդատների և մասնագիտական գործելակերպի վրա:

Սա սկսվում է ռիսկերի քարտեզագրման, միջադեպերի կառավարման, հանրային հաղորդակցության և մատակարարների կառավարման համար հստակորեն նշանակված պարտականություններից, որոնք բոլորը փաստաթղթավորված են գործնական, օգտագործելի պլաններով: Այս պլանները պետք է ներառվեն ամենօրյա պրակտիկայում՝ հիբրիդային սպառնալիքների սցենարներ մոդելավորող կանոնավոր վարժանքների միջոցով, ներառյալ արտահոսքի արձագանքման փորձնական ձեռնարկը՝ նախապես հաստատված հաղորդագրություններով և վարժանքից հետո շտկողական քայլերով, որոնց կատարումը վերահսկվում է մինչև ամբողջական ավարտը:

Տեխնոլոգիան և ընթացակարգերը պետք է հետևեն նախագծման պահից իսկ ներդրված անվտանգության սկզբունքներին, ինչպիսիք են նվազագույն արտոնություններով մուտքը, օգտատերերի և սարքերի անընդհատ ստուգումը և կարևորագույն գործողությունների համար անցանց պահուստավորումը՝ լարվածության պայմաններում շարունակականությունն ապահովելու համար: Գնումների չափորոշիչները պետք է պահանջեն անվտանգ մշակման պրակտիկայի ապացույցներ, միջադեպերի մասին արագ հաղորդելու և երրորդ կողմի բաղադրիչների թափանցիկության ապացույցներ՝ ձախողման մեկ կետից խուսափելու համար:

Առաջընթացի ցուցանիշներից են ավելի արագ հայտնաբերումը և զսպումը, ժամանակին և թափանցիկ հանրային թարմացումները, ինչպես նաև համապարփակ աուդիտի հետքերը, որոնք պարզաբանում են միջադեպերը՝ առանց զգայուն տեղեկատվությունը բացահայտելու:

2. **Ազգային աջակցության էկոհամակարգի խթանում.** Ներքին կարողությունները պետք է ամրապնդվեն ամուր, ամբողջ կառավարության ցանցով, քանի որ ոչ մի առանձին հաստատություն չի կարող հաջողության հասնել մեկուսացված:

Մշտական համագործակցության ցանցը պետք է գործի ամբողջ տարին՝ կապելով ընտրական մարմինը տեխնիկական, կարգավորող, անվտանգության և վերահսկողության գործընկերների հետ: Թեթև միաձուլված բջիջների մոդելը հնարավորություն է տալիս իրական ժամանակում տեղեկատվություն փոխանակել («միասին վերլուծել, գործել մանդատի շրջանակներում»), ապահովելով, որ բոլոր կողմերը ունենան ընդհանուր ըմբռնում՝ միաժամանակ պահպանելով գործառնական անկախությունը: Համատեղ ծառայությունները կարող են ներառել տեղական իշխանությունների և փոքր կազմակերպությունների համար նախատեսված օգնության գիծ, խոշոր առցանց հարթակներին արագ արձագանքման ալիքներ և կասկածելի աուդիո կամ վիդեո ստուգման մեխանիզմ՝ լրագրողներին և հանրությանը հեղինակավոր աղբյուրներին հասանելիություն ապահովելու համար:

Օրինական և համաչափ համագործակցությունը պետք է երաշխավորվի գրավոր ընթացակարգերի, պաշտոնով պայմանավորված հասանելիության և փոխանակված տեղեկատվության թափանցիկ գրանցումների միջոցով: Նման ցանցերը հնարավորություն

են տալիս ավելի վաղ միջգերատեսչական նախազգուշացումներ տալ, նվազեցնել աշխատանքի կրկնությունը և ամենակարևոր պահին նպաստել ավելի միատեսակ ու հետևողական հանրային ուղերձների տարածմանը:

3. **«Ամբողջ հասարակության» մոտեցում.** Ժողովրդավարական դիմակայունությունը կախված է անկախ լրատվամիջոցների, քաղաքացիական հասարակության, ակադեմիական աշխարհի, տեղական իշխանությունների, մասնավոր հատվածի և համայնքների ներգրավումից՝ գրագիտությունը, ստուգման մակարդակը և ներառական հանրային հաղորդակցությունը բարելավելու համար, որոնք իրականացվում են այնպիսի եղանակներով, որոնք պաշտպանում են իրավունքները, թափանցիկությունը և բազմակարծությունը:

Թափանցիկությունը պետք է դառնա ստանդարտ պրակտիկա՝ յուրաքանչյուր հիմնական գործընթացի համար նախատեսված, հեշտությամբ մատչելի վեբ էջերի միջոցով: Կանխարգելիչ հաղորդագրությունների օգտագործումը պետք է սահմանափակ լինի և համապատասխանեցվի ընտրական ցիկլին՝ կենտրոնանալով հստակ ազդանշանների վրա՝ ինչ ակնկալել, ինչպես ստուգել և որտեղ հաղորդել՝ հետևողականորեն ուղղորդելով լսարանին դեպի պաշտոնական աղբյուրները:

Վստահելի տեղական լրատվամիջոցներն ու կազմակերպությունները կարող են օգնել ընդլայնել լսարանը՝ տրամադրելով վերահրատարակման համար հարմար պատրաստի բացատրություններ: Անկախ լրատվամիջոցների և հետաքննող լրագրության աջակցությունը պետք է ընդլայնվի, բայց պահպանվի «ձեռքի մեկնած հեռավորության» սահմաններում՝ խմբագրական անկախությունը պաշտպանելու համար, ինչպես նաև լրացվի ոտնձգությունների, դոքսինգի և գենդերային բռնության դեմ պայքարի հստակ մեխանիզմներով: Մասնավոր մատակարարների հետ համագործակցությունը պետք է ապահովի զգայուն հարցումների անվտանգ ստուգում, վնասակար բովանդակության տարածման դեպքում արագ արձագանք և քաղաքական գովազդի շուրջ ավելի մեծ թափանցիկություն:

Վերջին հաշվով, այս մոտեցումը նպաստում է ավելի տեղեկացված և ներգրավված հանրության ձևավորմանը, լուրերի ավելի արագ շտկմանը և հուսալի տեղեկատվության ավելի լայն վերօգտագործմանը:

4. **Միջազգային համագործակցության և աջակցության մեխանիզմների ձևավորում.** Ազգային համակարգերը պետք է ինտեգրվեն միջսահմանային օգնության, ընդհանուր ստանդարտների և համատեղ գործողությունների հետ՝ հնարավորություն տալով աջակցության մասշտաբայնացման, երբ հարձակումները գերազանցում են ներքին կարողությունները:

Փոխօգնության պայմանավորվածությունները պետք է նախապես տեղի ունենան, որոնք կներառեն տեխնիկական արձագանքը, դատական աջակցությունը և հանրային հաղորդակցությունը ընտրությունների ժամանակահատվածում: Պետք է ստեղծվեն միջսահմանային հեռացումների կամ դրանց հետ կապված գործողությունների գործնական ուղիներ՝ նախապես հաստատված ձևանմուշներով՝ ուշացումները նվազագույնի հասցնելու համար: Ընտրություններին վերաբերող համակարգերի պաշտպանության և միջադեպերի բացահայտման ստանդարտ բազային սկզբունքները պետք է համաձայնեցվեն, և հնարավորության դեպքում պետք է կիրառվեն պաշտոնական լրատվամիջոցների համար բովանդակության ծագումնաբանության հիմնական պրակտիկաներ՝ ստուգումը հեշտացնելու և թափանցիկությունը բարձրացնելու համար:

Գիտելիքները պետք է փոխանցվեն նախնական փուլերից առաջ՝ փոխանակումների և գործուղումների միջոցով, մինչդեռ համագործակցության ցանցերը պետք է «համագործակցեն» արտասահմանյան գործընկերների հետ՝ ցուցանիշներ և ձեռնարկներ փոխանակելու համար: Արդյունքներն են՝ ավելի արագ օգնություն, երբ այն ամենակարևորն է, ավելի հստակ թարմացումներ տարբեր իրավասություններում և ավելի ուժեղ ապացույցներ, երբ պատասխանատվությունը վտանգված է, ինչը դիմակայունությունը վերածում է լեգիտիմության՝ թե՛ ներքին, թե՛ միջազգային գործընկերների հետ:

Բոլոր հակազդեցության միջոցները պետք է լինեն օրինական, անհրաժեշտ և համաչափ, ինչպես նաև հիմնված լինեն մարդու իրավունքների վրա հիմնված մոտեցման վրա: Գործնականում սա նշանակում է թիրախավորել մանիպուլյատիվ վարքագիծը՝ օրինական խոսքի փոխարեն, և առաջնահերթություն տալ գործընթացային միջոցներին՝ թափանցիկությանը, ծագմանը և հաշվետվողականությանը՝ բովանդակության հեռացման փոխարեն: Այն նաև ներառում է տվյալների նվազեցման և գաղտնիության նախագծմամբ ապահովման իրականացում. ժամանակով սահմանափակված, նպատակով սահմանափակված գործողությունների կիրառում՝ անկախ հսկողությամբ, աուդիտի հետքերով և բողոքարկման ուղիներով. և ակտիվ թափանցիկության պահպանում ճշմարտության կանոնական աղբյուրի միջոցով, որը հնարավորություն է տալիս հանրությանը ստուգել հավակնությունները:

Այս երաշխիքները համապատասխանում են տեղեկատվության հասանելիության երաշխիքներին (օրինակ՝ Tromsø Convention), խոսքի ազատության չափորոշիչներին (ICCPR/General Comment 34) և իրավունքները հարգող հարթակի կառավարմանը (DSA): Միևնույն ժամանակ, լրատվամիջոցների բազմակարծությունը և խմբագրական անկախությունը հակակշիռ են հանդիսանում գերհզորացմանը՝ ապահովելով, որ պաշտպանական միջոցառումները պաշտպանեն հենց այն ժողովրդավարական արժեքները, որոնք ընտրություններին ուղղված հիբրիդային սպառնալիքները փորձում են քայքայել:

Կառավարությունների և օրենսդիրների համար

1. **Ստեղծել և պահպանել ազգային ընտրական համագործակցության ցանց.** Այն դարձնել ազգային անվտանգության առաջնահերթություն՝ ստեղծելով պաշտոնական, մշտական մարմին, որը միավորում է ընտրությունների կազմակերպման մարմինը, կիբեռանվտանգության գործակալությունները, հետախուզական ծառայությունները, իրավապահ մարմինները և ռազմավարական հաղորդակցության ստորաբաժանումները: Այս ցանցը պետք է անընդհատ գործի՝ համատեղ ռիսկերի գնահատումներ անցկացնելու, սիմուլյացիոն վարժություններ անցկացնելու և համատեղ արձագանքման արձանագրություններ մշակելու համար:

2. **Ամրապնդել օրենսդրական և կարգավորող շրջանակները.**

    - **Քաղաքական գործընթացների ապօրինի ֆինանսավորում.** Եթե դեռևս դա նախատեսված չէ, արգելել քաղաքական գործիչներին անանուն և օտարերկրյա

նվիրատվությունները: Թարմացնել կանոնակարգերը՝ լուծելու կրիպտոարժույթների օգտագործման խնդիրը, բարձրացնելու առցանց գովազդի թափանցիկությունը և պահանջելու, որ քաղաքական նվիրատվությունները անցնեն պաշտոնական բանկային համակարգով՝ հետագծելիությունն ու վերահսկողությունը բարելավելու համար:

- **Հարթակի պատասխանատվություն.** Սոցիալական մեդիա հարթակների համար ներդնել և կիրառել ամուր կարգավորող շրջանակներ՝ կենտրոնանալով ալգորիթմական բովանդակության հավաքագրման, քաղաքական գովազդի և ստուգված հետազոտողների համար տվյալների հասանելիության թափանցիկության վրա:

- **Ընտրական և քրեական օրենսգրքեր.** Անցկացնել ընտրական իրավական շրջանակի համապարփակ վերանայում՝ հիբրիդային սպառնալիքների նկատմամբ խոցելի բացթողումները բացահայտելու և փակելու համար: Արդիականացնել քրեական օրենսգիրքը՝ հստակորեն սահմանելով և պատժելով ընտրական գործընթացին ուղղված հանցագործությունները, ինչպիսիք են համակարգված ապատեղեկատվական արշավները և ենթակառուցվածքների վրա կիբեռհարձակումները՝ արդյունավետ հետապնդում ապահովելու համար:

3. **Ներդրում կատարել ամբողջ հասարակության դիմակայունության ռազմավարության մեջ.** Երկակի մոտեցմամբ ֆինանսավորել և աջակցել ազգային նախաձեռնություններին, որոնք բարձրացնում են հանրային դիմակայունությունը: Նախ, հզորացնել քաղաքացիներին և քաղաքացիական հասարակությանը՝ ներդրումներ կատարելով երկարաժամկետ մեդիա և արհեստական բանականության գրագիտության արշավներում, ինչպես նաև ապահովելով կայուն աջակցություն բազմազան և անկախ մեդիա ոլորտին: Սրա կարևորագույն բաղադրիչը հետաքննող լրագրության համար հատկացվող ֆինանսավորումն է, որը կարևոր է հիբրիդային սպառնալիքների մեխանիզմները բացահայտելու համար: Երկրորդ, այս հասարակական ջանքերը պետք է լրացվեն կառավարության սեփական նախաձեռնողական հաղորդակցության հանձնառությամբ, որը կիրականացվի հավանական պատմությունների նախնական հերքման և պաշտոնական ճշմարտության աղբյուրների կենտրոնների ստեղծման միջոցով՝ հանրային տեղեկատվությունը կապելու և քաղաքացիներին մանիպուլյացիաներից պաշտպանելու համար:

4. **Ապահովել համատեղ տեխնիկական ենթակառուցվածք և ծառայություններ՝** Ստեղծել և ֆինանսավորել կենտրոնացված կարողություն՝ հիմնական ժողովրդավարական հաստատությունների համար համատեղ կիբեռանվտանգության և անվտանգ հաղորդակցման ծառայություններ մատուցելու համար: Սա պետք է ներառի կարևոր պաշտպանություններ, ինչպիսին է բաշխված ծառայությունը մերժելու (DDoS) հարձակումների մեղմացումը. ընտրությունների կազմակերպման մարմինների և այլ բարձր արժեք ունեցող թիրախների կայքերի համար՝ ապահովելով դրանց հասանելիությունը հանրության համար, հատկապես ճգնաժամերի ժամանակ:

EMB-ների համար

5. **Ընդունել կիբեռանվտանգության շարունակական դիրքորոշում.** Ընտրական անվտանգությունը դիտարկեք որպես ամբողջ տարվա գործընթաց: Ներդնել նախաձեռնողական պաշտպանության մոդել, որը ներառում է հիմնարար տեխնիկական վերահսկողության տեղակայում, ինչպիսիք են ֆիշինգին դիմացկուն բազմագործոն նույնականացումը բոլոր կարևոր հաշիվների համար, զրոյական վստահության կառուցվածքի կիրառում և բոլոր տեխնոլոգիական գնումներում նախագծային անվտանգության սկզբունքների պահանջ:

6. **Մշակել և փորձարկել ինտեգրված արձագանքման պլաններ.** Ստեղծել և պարբերաբար թարմացնել միջադեպերի արձագանքման պլաններ, որոնք համատեղում են տեխնիկական զսպումը ռազմավարական հաղորդակցության հետ: Հաստատությունները պետք է պատրաստ լինեն կիբեռ կամ տեղեկատվական

միջադեպի ժամանակ հանրության հետ հստակ և թափանցիկ շփվելու՝ ապատեղեկատվությունը կանխելու և վստահությունը պահպանելու համար:

Նման պլաններ մշակելու անհրաժեշտ առաջին քայլը թափանցիկ ներքին կառավարում ստեղծելն է՝ նշանակելով ավագ ղեկավար, որն ունի մանդատ և լիազորություն հավաքագրելու իրավաբանական, տեղեկատվական տեխնոլոգիաների և հաղորդակցությունների անձնակազմը և վերցնելու պատասխանատվության վերջնական պատասխանատվությունը միջադեպի ժամանակ պատասխանը կառավարելու համար: Այս ծրագրերը պետք է նաև պատրաստեն հաստատությանը թշնամական տեղեկատվության հրապարակումների: Սա ներառում է գաղտնազերծման ձեռնարկի մշակում, որը սահմանում է հստակ իրավական ընթացակարգեր՝ հաքերային հարձակման և արտահոսքի գործողության ժամանակային սղության պայմաններում տեղեկատվության նվազագույն վնասով բացահայտման համար՝ ապահովելով, որ գործակալությունը կարողանա արձագանքել վերահսկվող, իրավականորեն համապատասխան ձևով:

7. **Ակտիվորեն մասնակցել համագործակցության ցանցերին.** Լինել ներգրավված և հետևողական գործընկեր ազգային ընտրական համագործակցության ցանցի շրջանակներում: Օգտագործել այս ֆորումը՝ սպառնալիքների վերաբերյալ տեղեկատվություն փոխանակելու և ստանալու, ավելի լայն ռիսկերի մասին իրազեկվածություն ձևավորելու և անվտանգության և հետախուզական գործակալությունների հետ պաշտպանական գործողությունները համակարգելու համար:

Միջազգային աջակցության դերակատարների համար

8. **Խթանել «ցանցերի ցանցը».** Առաջնահերթություն տալ միջազգային համագործակցության շրջանակների ամրապնդմանը, ինչպիսիք են ԵՄ-ՆԱՏՕ համագործակցությունը և G7-ի արագ արձագանքման մեխանիզմը: Նպաստել ազգային համագործակցության ցանցերի միջև լավագույն փորձի և սպառնալիքների վերաբերյալ հետախուզության փոխանակմանը՝ ժողովրդավարական պաշտպանության գործնական կիրառման գլոբալ համայնք կառուցելու համար:

9. **Տրամադրել անհատականացված տեխնիկական և ռազմավարական աջակցություն՝** Առաջարկել նպատակային օգնություն գործընկեր երկրներին՝ նրանց օգնելու ստեղծել իրենց սեփական ազգային համագործակցության ցանցերը: Աջակցությունը պետք է հարմարեցվի ազգային համատեքստին և կենտրոնանա գործնական իրականացման վրա, ներառյալ համատեղ սիմուլյացիոն վարժանքների կազմակերպումը և մասնագիտացված ոլորտներում փորձագիտության տրամադրումը, ինչպիսիք են կիբեռանվտանգությունը և ֆինանսական բռնությունների դեմ պայքարը:

10. **Ընդունել մոդուլային ֆինանսավորման մոտեցում.** Աջակցությունը գործնական և արդյունքների վրա կենտրոնացած լինելն ապահովելու համար դոնորները պետք է դիտարկեն կոնկրետ, բարձր ազդեցություն ունեցող կարողությունների մոդուլների ֆինանսավորումը: Համատեղ ծառայությունների ոլորտում ռազմավարական ներդրումները կարող են ստեղծել մեծ մասշտաբի կարևորագույն տնտեսություն: Հիմնական մոդուլները կարող են ներառել՝

    - Ազգային ընտրական համագործակցության ցանցի քարտուղարություն՝ համակարգումը կառավարելու համար:

    - Կիբեռանվտանգության հիմնական փաթեթ՝ ընտրական մարմնի և այլ կարևորագույն գործակալությունների կայքերի համար DDoS հարձակումներից պաշտպանության նման համատեղ ծառայություններ մատուցելու համար:

    - Հաստատության մակարդակով կարողությունների փաթեթներ՝ հիմնական հաստատություններում ճշմարտության աղբյուրի կենտրոնների և միջադեպերին արձագանքման ձեռնարկների ստեղծման ֆինանսավորման համար:

- Հյուրընկալող երկրի պատրաստակամությունը միջազգային աջակցության համար՝ ճգնաժամի ժամանակ փորձագիտական օգնություն ստանալու համար իրավական, կազմակերպչական և տեխնիկական հիմքերը պատրաստելու համար, ինչպիսիք են նշանակված ազգային կապի կետը և նախապես հաստատված իրավական ձևանմուշները:

- Մասնագիտացված միջազգային արագ արձագանքման թիմեր՝ բարդ հիբրիդային սպառնալիքների մարտավարությունների կառավարման համար տեղակայելի, մասնագիտացված փորձագիտություն ապահովելու համար, օրինակ՝ կիբեռհարձակումներին արձագանքող, հաքերային հարձակումների և տվյալների արտահոսքի գործողություններին արձագանքող կամ ռազմավարական հաղորդակցման աջակցություն առաջարկող նվիրված թիմեր: Աջակցությունը պետք է լինի գործնական, պահանջարկի վրա հիմնված և կենտրոնացած լինի իրական համագործակցության վրա:

Սակայն, վերջին հաշվով, երկարաժամկետ հաջողությունը կայանում է սպառնալիքների իրականացումն ի սկզբանե կանխելու մեջ: Սրան կարելի է հասնել միայն գործառնական գերազանցության միջոցով՝ ընտրական գործընթացները անթերի անցկացնելով, արմատական թափանցիկությամբ շփվելով և սխալները ազնվորեն ընդունելով: Հենց կայուն ինստիտուցիոնալ կարողությունների և դժվարությամբ նվաճված հանրային վստահության կառուցման այս կայուն աշխատանքն է, որը կազմում է ամենաուժեղ պաշտպանությունը նրանց դեմ, ովքեր փորձում են խաթարել ժողովրդավարական գործընթացը:

07 Հղումներ

Agrawal, H., Hamada, Y., & Fernández Gibaja, U. (2021). *Regulating Online Campaign Finance: Chasing the Ghost?* International IDEA. https://www.idea.int/publications/catalogue/regulating-online-campaign-finance

Alihodžić, S. (2023): *Protecting elections: Risk management, resilience-building and crisis management in elections.* International IDEA. https://www.idea.int/publications/catalogue/protecting-elections-risk-management-resilience-building-and-crisis

Alliance for Securing Democracy. (2019). Russian hackers behind surge in cyberattacks targeting Ukrainian election. https://securingdemocracy.gmfus.org/incident/russian-hackers-behind-surge-in-cyberattacks-targeting-ukrainian-election/

Anghel, V. (2024). Why Romania just cancelled its presidential election. *Journal of Democracy* (online exclusive). https://www.journalofdemocracy.org/online-exclusive/why-romania-just-canceled-its-presidential-election/

Antoniuk, D. (2023, January 7). Moldova's government hit by flood of phishing attacks. *The Record*. https://therecord.media/moldovas-government-hit-by-flood-of-phishing-attacks

Antoniuk, D. (2024, October 21). 'Unprecedented' interference targets Moldova's elections. *The Record / Recorded Future News*. https://therecord.media/unprecedented-interference-moldova-elections-cyberattack

Antoniuk, D. (2025, September 22). Russia steps up disinformation efforts to sway Moldova's parliamentary vote. *The Record*. https://therecord.media/russia-steps-disinfo-moldova-election

Atlantic Council. (2018, September 11). Defining Russian election interference: An analysis of select 2014–2018 cyber-enabled incidents. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/defining-russian-election-interference-an-analysis-of-select-2014-to-2018-cyber-enabled-incidents-2/

Atlantic Council. (2023, February 24). *Narrative warfare: How the Kremlin and Russian news outlets justified a war of aggression against Ukraine*. https://www.atlanticcouncil.org/wp-content/uploads/2023/02/Narrative-Warfare-Final.pdf

Atlantic Council / DFRLab. (2024, November 4). Trends in China's US election interference illustrate its longer game. https://dfrlab.org/2024/11/04/china-us-election-interference/

Bakken, M. (2025, February 3). Election observation and hybrid threats. *European Democracy Hub*. https://europeandemocracyhub.epd.eu/election-observation-and-hybrid-threats/

Balmforth, T., & Dysa, Y. (2024, November 2). Moldova says Russia plans to disrupt expatriate voting in Sunday's runoff. *Reuters.* https://www.reuters.com/world/europe/moldova-claims-russia-plans-disrupt-expatriate-voting-sundays-runoff-2024-11-02/

Barata, J., & Lăzăr, E. (2025, January 27). Will the DSA save democracy? The test of the recent presidential election in Romania. *Tech Policy Press.* https://techpolicy.press/will-the-dsa-save-democracy-the-test-of-the-recent-presidential-election-in-romania

Bateman, J., & Jackson, D. (2024). *Countering disinformation effectively: An evidence-based policy guide.* Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/05/countering-disinformation-effectively-policy-guide

Bay, S. (2024). *Countering hybrid threats to elections: From updating legislation to establishing collaboration networks* (Hybrid CoE Research Report 12). Hybrid CoE https://www.hybridcoe.fi/publications/hybrid-coe-research-report-12-countering-hybrid-threats-to-elections-from-updating-legislation-to-establishing-collaboration-networks/

Bay, S. (2025). *Protecting electoral integrity: The case of Sweden*. International IDEA. https://www.idea.int/publications/catalogue/protecting-electoral-integrity-case-sweden

Bay, S., Appelgren, J., Isakson, E., Lindgren, J., & Thunholm, P. (2022). *Threats to Swedish public elections – Examples and scenarios for the Election Administration* (FOI-R--5298--SE). FOI. https://foi.se/en/foi/reports/report-summary.html?reportNo=FOI-R--5298--SE

Bing, C., & Vicens, A. J. (2024, October 23). Iranian hacker group aims at US election websites and media before vote, Microsoft says. *Reuters.* https://www.reuters.com/technology/cybersecurity/iranian-hacker-group-focuses-us-election-websites-media-ahead-vote-microsoft-2024-10-23/

Bjola, C. (2025, February 7). Algorithmic invasions: How information warfare threatens NATO's eastern flank. *NATO Review.* https://archives.nato.int/nato-review-algorithmic-invasions-how-information-warfare-threatens-natos-eastern-flank

Brennan Center for Justice. (2020, October). *2020's lessons for election security.* https://www.brennancenter.org/our-work/research-reports/2020s-lessons-election-security

Bryjka, F. (2024). Russian interference nearly overwhelmed Moldovan presidential election–referendum vote. *Polish Institute of International Affairs (PISM).* https://pism.pl/publications/russian-interference-nearly-overwhelmed-moldovan-presidential-election-referendum-vote

C2PA. (2024). Content credentials & C2PA overview. https://c2pa.org

Canada (Government of Canada). (2025, July 8). *Multi-stakeholder insights: A compendium on countering election interference.* https://www.canada.ca/en/democratic-institutions/services/paris-call-trust-security-cyberspace/multistakeholder-insights-compendium-countering-election-interference.html

The Carter Center. (2025, July 8). Democracy program. https://www.cartercenter.org/peace/democracy/

Center for an Informed Public, Digital Forensic Research Lab, Graphika, & Stanford Internet Observatory. (2021). *The long fuse: Misinformation and the 2020 election.* Election Integrity Partnership. https://purl.stanford.edu/tr171zs0069

Center for Internet Security. (2025a, July 8). EI-ISAC. https://www.cisecurity.org/ei-isac

Center for Internet Security. (2025b, July 8). The IT lifecycle – The CIS guide to election technology procurements. https://election-procurement.docs.cisecurity.org/en/latest/IT_product_services_lifecycle.html

Center for Internet Security. (2025c). Election security spotlight – DDoS attacks. https://www.cisecurity.org/insights/spotlight/election-security-spotlight-ddos-attacks

Cerulus, L. (2025, June). EU comes to Moldova's defense against Russian hacking. *POLITICO*. https://www.politico.eu/article/eu-moldova-election-cyber-security-russia-hacking/

Chainalysis. (2024a). *2024 cryptocurrency adoption index.* https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/

Chainalysis. (2024b). Malign Interference and Crypto: How Crypto Transaction Tracing Can Expose and Disrupt Malign Influence Efforts. https://www.chainalysis.com/blog/malign-interference-and-crypto/

Chan, K. (2024, December 17). EU investigates TikTok over Romanian presidential election safeguards. *AP News.* https://apnews.com/article/0638e90cb3898fc61619e8aed4731a53

Chan, K. (2025, July 25). Meta will cease political ads in European Union by fall, blaming bloc's new rules. *AP News.* https://apnews.com/article/meta-instagram-facebook-eu-european-union-political-89efeac96723308d2a0469740d24d433

CISA (Cybersecurity and Infrastructure Security Agency). (2024a, January 18). *Risk in focus: Generative A.I. and the 2024 election cycle.* https://www.cisa.gov/resources-tools/resources/risk-focus-generative-ai-and-2024-election-cycle

CISA. (2024b). #Protect2024: Election security. https://www.cisa.gov/topics/election-security/protect2024

CISA. (2025, July 8). Join the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). https://www.cisa.gov/resources-tools/groups/join-elections-infrastructure-information-sharing-and-analysis-center-ei-isac

CISA, & EAC. (2024a). *Election infrastructure incident response communications guide.* https://www.eac.gov/sites/default/files/2024-10/Election_Infrastructure_Incident_Response_Comms_Guide_508.pdf

CISA, & EAC. (2024b). *Enhancing election security through public communications.* https://www.eac.gov/sites/default/files/2024-06/Enhancing_Election_Security_Through_Public_Communications.pdf

Cisco (Outshift). (2025, July 8). Top 15 software supply chain attacks: Case studies. https://outshift.cisco.com/blog/top-10-supply-chain-attacks

Clayton, M. (2014, June 17). Ukraine election narrowly avoided 'wanton destruction' from hackers. *The Christian Science Monitor.* https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers

Cloudflare. (2025, July 8). Exploring Internet traffic shifts and cyber attacks during the 2024 US election. https://blog.cloudflare.com/exploring-internet-traffic-shifts-and-cyber-attacks-during-the-2024-us-election/

CNN. (2024a, April 26). Cyberattack forces Georgia county to sever connection to state voter registration system. https://edition.cnn.com/2024/04/26/politics/georgia-coffee-county-cyberattack-voter-system/index.html

CNN. (2024b, August 19). US concludes Iran is behind hacking attempts targeting Trump and Biden-Harris campaigns. https://edition.cnn.com/2024/08/19/politics/us-concludes-iran-behind-trump-biden-harris-hacking/index.html

Coherent Market Insights. (2025, March 17). Crypto exchange market size and forecast, 2025–2032. https://www.coherentmarketinsights.com/industry-reports/crypto-exchange-market

CoinGecko. (2025). Cryptocurrency prices, charts and market capitalizations. https://www.coingecko.com

Columbia University, SIPA IGP. (2025, July 8). French official outlines government approach to countering foreign online operations. https://igp.sipa.columbia.edu/news/french-official-outlines-government-approach-countering-foreign-online-operations

Communications Security Establishment Canada. (2025, March). CSE releases 2025 update to report on cyber threats to Canada's democratic process. https://www.canada.ca/en/communications-security/news/2025/03/communications-security-establishment-canada-releases-2025-update-to-report-on-cyber-threats-to-canadas-democratic-process.html

Constella Intelligence. (2025, July 8). Voter database leaks threaten the 2024 U.S. election. https://constella.ai/2024-u-s-election-voter-database-leaks/

Council of Europe. (2024). Internet voting in post-war elections in Ukraine: risks and challenges – results of the study presented. https://www.coe.int/en/web/kyiv/-/internet-voting-in-post-war-elections-in-ukraine-risks-and-challenges-results-of-the-study-presented

Council of Europe. (2025, July 8). Foreign interference in electoral processes at local and regional levels. https://rm.coe.int/0900001680b4cb53

County of San Luis Obispo, Clerk-Recorder. (2024, August 1). Federal agencies say cyber attack could hinder public access to election information, not election itself. https://www.slocounty.ca.gov/departments/clerk-recorder/news-announcements/federal-agencies-say-cyber-attacks-could-hinder-public-access-to-election-information-but-not-to-ele

CrowdStrike. (2025a). Zero Trust Security Explained: Principles of the Zero Trust Model. https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/

CrowdStrike. (2025b). Press release: CrowdStrike releases 2025 threat hunting report. https://www.crowdstrike.com/en-us/press-releases/crowdstrike-releases-2025-threat-hunting-report/

Csernatoni, R. (2024). Can democracy survive the disruptive power of AI? *Carnegie Endowment.* https://carnegieendowment.org/research/2024/12/can-democracy-survive-the-disruptive-power-of-ai

Cyble. (2024). EU cybersecurity in 2024: Insights from ENISA's latest report. https://cyble.com/blog/eu-cybersecurity-in-2024-insights-from-enisa-latest-report/

Cyble. (2025, July 8). Software supply chain attacks surged in April and May. https://cyble.com/blog/supply-chain-attacks-surge-in-april-may-2025/

Deloitte. (2024). ENISA threat landscape 2024: Cyber threat landscape in the financial sector. https://www.deloitte.com/ro/en/our-thinking/articles/raportul-enisa-threat-landscape-2024-peisajul-amenintarilor-cibernetice-sectorul-financiar.html

Electoral Commission (UK). (2024). Electoral Commission response to cyber-attack attribution. https://www.electoralcommission.org.uk/media-centre/electoral-commission-response-cyber-attack-attribution-0

Elections Canada. (2025, July 8). Our work with security agencies and partners – Media guide for the 45th general election. https://www.elections.ca/content.aspx?section=med&dir=guide&document=p19&lang=e

Electionline. (2024, October). 2024 election threat landscape. https://electionline.org/wp-content/uploads/2024/10/2024-Election-Threat-Landscape-TLP-CLEAR.pdf

ENISA / NIS Cooperation Group. (2024). *Compendium on elections cybersecurity and resilience.*

Press release: https://www.enisa.europa.eu/news/safeguarding-eu-elections-amidst-cybersecurity-challenges

Euromaidan Press. (2014). Russian hacking attempt fails, but fake election news airs. https://euromaidanpress.com/2014/05/26/russian-hacking-attempt-fails-but-fake-election-news-airs/

European Commission. (2016). *Joint framework on countering hybrid threats: A European Union response* (JOIN(2016) 18 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52016JC0018

European Commission. (2024). Commission opens formal proceedings against TikTok under the DSA (IP/24/6487). https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487

European Commission. (2025a). Hybrid threats – Defence Industry and Space. https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en

European Commission. (2025b). European cooperation network on elections. https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/european-cooperation-network-elections_en

European Commission. (2025c, June 12). Commission services and Moldovan authorities conduct a stress test on potential digital hybrid threats to election integrity ahead of Moldova's parliamentary elections. *Shaping Europe's Digital Future.* https://digital-strategy.ec.europa.eu/en/news/commission-services-and-moldovan-authorities-conduct-stress-test-potential-digital-hybrid-threats

European Digital Media Observatory (EDMO). (2024). *Final report – Outputs and outcomes of a community-wide effort (EP elections).* https://edmo.eu/publications/final-report-results-and-outcomes-of-a-community-wide-effort/

European External Action Service (EEAS). (2024). *Second EEAS report on Foreign Information Manipulation and Interference (FIMI) threats.* https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

European External Action Service (EEAS). (2025a). *Third EEAS report on Foreign Information Manipulation and Interference (FIMI) threats.* https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

European External Action Service (EEAS). (2025b). Information integrity and countering FIMI. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

European External Action Service (EEAS). (2025c). About the EU Partnership Mission in the Republic of Moldova (EUPM Moldova). https://www.eeas.europa.eu/eupm-moldova/about-eu-partnership-mission-republic-moldova_en

EUvsDisinfo. (2024a). *Doppelgänger strikes back: FIMI activities targeting European Parliament elections.* https://euvsdisinfo.eu/doppelganger-strikes-back-unveiling-fimi-activities-targeting-european-parliament-elections/

EUvsDisinfo. (2024b). Who is afraid of the European Moldova? https://euvsdisinfo.eu/who-is-afraid-of-the-european-moldova/

Europol. (2025, February 28). The DNA of organised crime is changing – and so is the threat to Europe. https://www.europol.europa.eu/media-press/newsroom/news/dna-of-organised-crime-changing-and-so-threat-to-europe

FBI. (2024, November 5). Statement on bomb threats to polling locations. https://www.fbi.gov/news/press-releases/fbi-statement-on-bomb-threats-to-polling-locations

Forbes. (2025, March 10). AI-driven phishing and deepfakes: The future of digital fraud. https://www.forbes.com/councils/forbestechcouncil/2025/03/10/ai-driven-phishing-and-deep-fakes-the-future-of-digital-fraud/

Freedom House. (2024). *Freedom in the world 2024: The mounting damage of flawed elections and armed conflict.* https://freedomhouse.org/report/freedom-world/2024/mounting-damage-flawed-elections-and-armed-conflict

GAO (US Government Accountability Office). (2020, February). *Election security: DHS plans are urgently needed…* https://www.gao.gov/assets/gao-20-267.pdf

Gavin, W. (2025, September 23). Moldova arrests 74 in plot to disrupt election. *BBC News.* https://www.bbc.com/news/articles/c4g5kl0n5d2o

Gilbert, D. (2024, April 11). Election workers are already burned out—and on high alert. *WIRED*. https://www.wired.com/story/election-officials-threats-disinformation/

Global Witness. (2024, December 6). TikTok pushes far-right candidate content in Romanian election, investigation shows. https://www.globalwitness.org/en/press-releases/tiktok-pushes-far-right-candidate-content-romanian-election-global-witness-investigation-shows/

Global Witness. (2025, May 15). Ahead of the second round, TikTok continues to push far-right content in Romania. https://globalwitness.org/en/campaigns/digital-threats/tiktok-algorithm-continues-to-push-multiple-times-more-far-right-content-to-users-ahead-of-romanian-election/

Google Cloud. (2023, August). *Poll Vaulting: Cyber Threats to Global Elections.* https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-global-elections

Google DeepMind. (2025). SynthID – A tool to watermark and identify content generated through AI. https://deepmind.google/science/synthid/

Hedenskog, J., & Hjelm, M. (2020, October 25). Propaganda by Proxy: Ukrainian oligarchs, TV and Russia's influence (FOI Memo 7312). FOI. https://www.foi.se/rest-api/report/FOI%20Memo%207312

Hedling, E. (2025, April 15). *Social identities and democratic vulnerabilities: Learning from examples of targeted disinformation* (Hybrid CoE Paper 24). Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2025/04/20250415-Hybrid_CoE_Paper-24-WEB.pdf

Hoffman, F. G. (2022). *Towards a fifth wave of deterrence theory and practice* (Hybrid CoE Paper 12). Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/

Hollis, D. B., & Ohlin, J. D. (2021). *Defending democracies: Combating foreign election interference in a digital age.* Oxford University Press. https://global.oup.com/academic/product/defending-democracies-9780197556979

Hoogensen Gjørv, G., & Jalonen, O. (2023). *Identity as a tool for disinformation* (Hybrid CoE Strategic Analysis 34). Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-34-identity-as-a-tool-for-disinformation-exploiting-social-divisions-in-modern-societies/

Hoxhunt. (2025, July 8). AI-powered phishing outperforms elite cybercriminals in 2025. https://hoxhunt.com/blog/ai-powered-phishing-vs-humans

Huo, J. (2024, November 12). Foreign influence efforts reached a fever pitch during the 2024 elections. *NPR*. https://www.npr.org/2024/11/09/nx-s1-5181965/2024-election-foreign-influence-russia-china-iran

Hybrid CoE. (2024, January). Frequently asked questions on hybrid threats. https://www.hybridcoe.fi/wp-content/uploads/2024/01/FAQ-on-Hybrid-Threats.pdf

Hybrid CoE. (2025). Hybrid threats. https://www.hybridcoe.fi/hybrid-threats/

International Foundation for Electoral Systems (IFES). (2024, December 20). The Romanian 2024 election annulment: Addressing emerging threats to electoral integrity. https://www.ifes.org/publications/romanian-2024-election-annulment-addressing-emerging-threats-electoral-integrity

IGP (General Inspectoratul al Poliției). (2025, September 22). Trust Media responsabil de propaganda pro-rusă și dezinformare, finanțat printr o schemă complexă de spălare de bani, vizat în perchezițiile de astăzi. *Poliția Republicii Moldova.* https://www.igp.gov.md/ro/politia-actiune/trust-media-responsabil-de-propaganda-pro-rusa-si-dezinformare-finantat-printr-o

IGP (General Inspectoratul al Poliției). (2025, August 13). Autoritățile intensifică țiuunile împotriva dezinformării in space digital: peste 400 de canale TikTok vizate pentru blocare. *Poliția Republicii Moldova*. https://politia.md/ro/noutati/autoritatile-intensifica-actiunile-impotriva-dezinformarii-spatiul-digital-peste-400-de

International IDEA. (2019). Inter-agency Collaboration on Cybersecurity in Elections: Roundtable Discussion. https://www.idea.int/news/inter-agency-collaboration-cybersecurity-elections-roundtable-discussion

International IDEA. (2023, November 28). Mauritius: Inter-agency collaboration against hybrid threats. https://www.idea.int/news/mauritius-inter-agency-collaboration-against-hybrid-threats

International IDEA. (2024, September 17). The Global State of Democracy 2024: Strengthening the legitimacy of elections in a time of radical uncertainty. https://www.idea.int/publications/catalogue/global-state-democracy-2024-strengthening-legitimacy-elections

International IDEA. (2025). Political finance database. https://www.idea.int/data-tools/data/political-finance-database

ISACA. (2025, July 8). The 2025 software supply chain security report. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/the-2025-software-supply-chain-security-report

Ivanti. (2025, July 8). Software supply chain attacks risk on the rise. https://www.ivanti.com/blog/software-supply-chain-attack-risk

Kovalčiková, N., & Spatafora, G. (2024, December 17). The future of democracy: Lessons from the US fight against foreign electoral interference in 2024 (EUISS Brief). *EU Institute for Security Studies.* https://www.iss.europa.eu/publications/briefs/future-democracy-lessons-us-fight-against-foreign-electoral-interference-2024

Kubica, L. (2024). *Moldova's struggle against Russia's hybrid threats* (Hybrid CoE Working Paper 28). Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-28-moldovas-struggle-against-russias-hybrid-threats-from-countering-the-energy-leverage-to-becoming-more-sovereign-overall/

Ledford, H. (2024). Deepfakes, trolls and cybertroopers: How social media could sway elections in 2024. *Nature,* 626(7902), 463–464. https://www.nature.com/articles/d41586-024-00274-7

Levin, D. H. (2020). *Meddling in the ballot box: The causes and effects of partisan electoral interventions.* Oxford University Press. https://academic.oup.com/book/36920

Lewandowsky, S., Cook, J., Ecker, U. K. H., Albarracín, D., Amazeen, MA, Kendeou, P., & Zaragosa, MS (2020). *The Debunking Handbook 2020.* https://www.climatechangecommunication.org/wp-content/uploads/2020/10/DebunkingHandbook2020.pdf

Liberties (Civil Liberties Union for Europe). (2025). *Rule of law report 2025*. https://dq4n3btxmr8c9.cloudfront.net/files/vdxw3e/Liberties_Rule_of_Law_Report_2025_v.pdf

Lopatka, J. (2024, March 27). Czechs sanction Medvedchuk, website over pro-Russian EU political influence. *Reuters*. https://www.reuters.com/world/europe/czechs-sanction-medvedchuk-website-over-pro-russian-eu-political-influence-2024-03-27/

Lores, R. (2025). *Global Crypto User Index 2025*. Statista. https://www.statista.com/outlook/fmo/digital-assets/cryptocurrencies/worldwide?srsltid=AfmBOorgqEAOLng7cSMAFDInxing0Kw13xMpvwg1gJcvm_ZC590gOuQg

Martin, T. (2022, November 11). Russia's cyberattacks aimed at 'destabilizing' Moldova, PM says. *The Record.* https://therecord.media/russias-cyberattacks-aimed-at-destabilizing-moldova-pm-says

McGrath, S. (2025, September 22). Moldova says it has foiled a Russian-backed plot to disrupt its parliamentary election. *AP News.* https://apnews.com/article/moldova-russia-arrests-plot-election-293ee902e878ce1efcca339759eb06d0

McGrath, S., & Alexandru, A. (2025, September 9). Moldova's president accuses Russia of conducting 'hybrid war' ahead of key elections. *AP News.* https://apnews.com/article/moldova-elections-russia-influence-europe-8cc882551dd52957491e3cfd112cc878

McGrath, S., & Dumitrache, N. (2025, May 13). Romania's redo of a presidential election is a high-stakes test of a battered democracy. *AP News.* https://apnews.com/article/romania-constitutional-court-annuls-election-2nd-round-6e5a089462c10f5079e0812c908736aa

Meaker, M. (2023, October 3). Slovakia's election deepfakes show AI is a danger to democracy. *WIRED.* https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy/

Microsoft. (2025, October). *Microsoft Digital Defense Report 2025.* https://aka.ms/Microsoft-Digital-Defense-Report-2025#page=1

Microsoft Threat Analysis Center. (2024a, April 4). Same targets, new playbooks: East Asia threat actors employ unique methods. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/east-asia-threat-actors-employ-unique-methods

Microsoft Threat Analysis Center. (2024b, September 27). Russia-linked operators engaged in expansive efforts to influence US voters. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/russia-linked-operators-engaged-in-expansive-efforts-to-influence-us-voters

Molas, B. (2024, December 15). Doxing: A literature review. *The International Centre for Counter-Terrorism.* https://icct.nl/publication/doxing-literature-review

Moldpres – State News Agency. (2025, August 13). Moldova's Intelligence and Security Service, Police, ANRCETI ask to block over 400 TikTok channels. https://www.moldpres.md/eng/society/moldova-s-intelligence-and-security-service-police-anrceti-ask-to-block-over-400-tiktok-channels

Militära underrättelse- och säkerhetstjänsten (Must). (2025). *Annual Report 2024.* https://www.forsvarsmakten.se/contentassets/546bbe13064a4c739e1cbc4b5e4571f7/2024-must-annual-report.pdf

Nakamura, D., Belton, C., & Sommer, W. (2024, September 4). Justice Dept. charges two Russian media operatives in alleged scheme. *The Washington Post.* https://www.washingtonpost.com/national-security/2024/09/04/justice-department-election-security/

Nardelli, A. (2025, September 22). Revealed: Putin's secret plan to hack Moldova's pivotal election. *Bloomberg.* https://www.bloomberg.com/news/articles/2025-09-22/moldova-elections-russia-s-plan-to-hack-the-vote

National Task Force on Election Crises. (2025a, July 8). National Task Force on Election Crises. Protect Democracy. https://protectdemocracy.org/work/national-task-force-on-election-crises/

National Task Force on Election Crises. (2025b, July 8). Lessons from the 2024 general election. https://electiontaskforce.org/lessons-from-the-2024-general-election/

NATO. (2022). *Strategic concept.* https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO. (2024). Countering hybrid threats. https://www.nato.int/cps/en/natohq/topics_156338.htm

NATO. (2025). NATO's approach to counter information threats (official text). https://www.nato.int/cps/en/natohq/official_texts_231905.htm

NCSC (UK). (2025). *Cyber Assessment Framework v4.0.* https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf

Newman, N., Fletcher, R., Robertson, C. T., Ross Arguedas, A., & Nielsen, R. K. (2024). *Digital News Report 2024.* Reuters Institute. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf

National Institute of Standards and Technology (NIST). (2020). *SP 800-207: Zero Trust Architecture.* https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

National Institute of Standards and Technology (NIST). (2022). *SP 800-218: Secure Software Development Framework (SSDF)* v1.1. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-218.pdf

National Institute of Standards and Technology (NIST). (2023). *SP 800-207A: A Zero Trust Architecture model for access decisions.* https://csrc.nist.gov/pubs/sp/800/207/a/final

National Institute of Standards and Technology (NIST). (2024). *SP 800-218A: Secure software development practices for generative AI & dual-use foundation models.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218A.pdf

O'Brien, M., & Swenson, A. (2024, February 16). Tech companies sign accord to combat AI-generated election trickery. *AP News.* https://apnews.com/article/ai-generated-election-deepfakes-munich-accord-meta-google-microsoft-tiktok-x-c40924ffc68c94fac74fa994c520fc06

Ohlin, J. D. (2020). *Election interference: International law and the future of democracy.* Cambridge University Press. https://doi.org/10.1017/9781108859561

Olari, V. (2024, October 18). What to know about Russian malign influence in Moldova's upcoming election. *Atlantic Council.* https://www.atlanticcouncil.org/blogs/new-atlanticist/what-to-know-about-russian-malign-influence-in-moldovas-upcoming-election/

Olari, V. (2025a, March 6). Telegram network seeks to manipulate Moldova's local political discourse. *DFRLab.* https://dfrlab.org/2025/03/06/telegram-network-moldova/

Olari, V. (2025b, March 26). Cross-platform campaign sows anti-Europe division in Moldova. *DFRLab.* https://dfrlab.org/2025/03/26/cross-platform-campaign-sows-anti-europe-division-in-moldova/

OSCE/ODIHR. (2017). *Montenegro, Parliamentary Elections, 16 Oct 2016: Final report.* https://www.osce.org/odihr/elections/montenegro/295511

OSCE/ODIHR. (2021). *Republic of Moldova, Early Parliamentary Elections, 11 July 2021: Final report.* https://www.osce.org/odihr/elections/moldova/501518

OSCE/ODIHR. (2024). *Moldova, Presidential Election and Constitutional Referendum, 20 Oct 2024: Statement of preliminary findings and conclusions.* https://www.osce.org/odihr/elections/moldova/578815

OSCE/ODIHR. (2025a, February 20). *Poland, Presidential Election, Run-off, 2025: Final report.* https://www.osce.org/odihr/elections/poland/591761

OSCE/ODIHR. (2025b, September 28). *Republic of Moldova, statement of preliminary findings and conclusions.* https://www.osce.org/files/f/documents/4/7/597800.pdf

OSCE/ODIHR. (2025c, March 14). Republic of Moldova: *Presidential election and constitutional referendum, 20 Oct & 3 Nov 2024, Final report.* https://www.osce.org/files/f/documents/3/9/587451_0.pdf

OSCE/ODIHR. (2025d, May 5). Notable efforts to address electoral integrity but certain aspects… (Romania). https://www.osce.org/odihr/elections/romania/590330

Pamment, J., Nothaft, H., Agardh-Twetman, H. & Fjällhed, A. (2018). *Countering Information Influence Activities: The State of the Art.* MSB. https://rib.msb.se/filer/pdf/28697.pdf

Pamment, J., & Tsurtsumia, D. (2025, May). Beyond Operation Doppelgänger: A capability assessment of the Social Design Agency (SDA). Lund University & Swedish Psychological Defence Agency. https://www.psychologicaldefence.lu.se/sites/psychologicaldefence.lu.se/files/2025-05/Beyond%20Operation%20Doppelg%C3%A4nger.pdf

Pamment, J., & Isaksson, E. (2024). *Psychological Defence: Concepts and Principles for the 2020s* (MPF Report Series 6/2024). Lund University & Swedish Psychological Defence Agency. https://www.mpf.se/wp-content/uploads/2024/03/mpf_rapport_6_2024_psychological_defence.pdf

Perdomo, C., & Uribe Burcher, C. (2017). Money, influence, corruption and capture: can democracy be protected? *The Global State of Democracy 2017 Exploring Democracy's Resilience. International IDEA.* https://www.idea.int/gsod-2017/files/IDEA-GSOD-2017-REPORT-EN.pdf

Popescu-Zamfir, R. (2025, September 26). *Moldova's Election Is a Test for Russian Influence in Europe. Carnegie Endowment for International Peace.* https://carnegieendowment.org/research/2025/09/moldovas-election-is-a-test-for-russian-influence-in-europe?lang=en

Posetti, J., et al. (2020). *Online violence against women journalists: A global snapshot of incidence and impacts.* UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000375136/PDF/375136eng.pdf.multi

Rainsford, S. (2024, December 4). Romania hit by major election influence campaign and Russian cyber-attacks. BBC: https://www.bbc.com/news/articles/cgq18w507dko

ReliaQuest. (2024, September 24). 2024 US election: Top cyber threats & organizational impacts. https://www.reliaquest.com/blog/2024-us-election-top-cyber-threats-organizational-impacts/

Reuters. (2024a, October 24). Chinese influence operation targets U.S. down-ballot races, Microsoft says. https://www.reuters.com/world/us/chinese-influence-operation-targets-us-down-ballot-races-microsoft-says-2024-10-23/

Reuters. (2024b, November 5). Hoax bomb threats linked to Russia target polling places in battleground states, FBI says. https://www.reuters.com/world/us/fake-bomb-threats-linked-russia-briefly-close-georgia-polling-locations-2024-11-05/

RFE/RL Moldovan Service. (2024, October 25). Moldovan police accuse pro-Russian oligarch of $39M vote-buying scheme. https://www.rferl.org/a/moldova-police-accuse-shor-russia-oligarch-39m-vote-buying/33172951.html

Roth, A. (2024, September 4). Russia accused of trying to influence US voters through online campaign. *The Guardian.* https://www.theguardian.com/us-news/2024/sep/04/russia-us-election-online-campaign-sanctions

Saeva, E., & Tasheva, I. (2024). The 2024 EU elections and cybersecurity: A retrospective and lessons learned. *European View* (Martens Centre). https://www.martenscentre.eu/wp-content/uploads/2024/11/12.pdf

Schroeder, DT, Cha, M., Baronchelli, A., Bostrom, N., Christakis, NA, Garcia, D., … Kunst, JR. (2025). How malicious AI swarms can threaten democracy. arXiv. https://doi.org/10.48550/arXiv.2506.06299

Stimson Center. (2024, August 8). RAI Session: AI & democracy (event). https://www.stimson.org/event/rai-session-ai-democracy/

Stockwell, S., Hughes, M., Swatton, P., Zhang, A., Hal, J., & Kieran. (2024). *AI-enabled influence operations: Safeguarding future elections.* The Alan Turing Institute (CETaS). https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-safeguarding-future-elections

Tanas, A. (2024, October 24). Moldovan president says bribery affected election, pledges run-off vote. *Reuters.* https://www.reuters.com/world/europe/moldova-police-say-businessman-shor-channelled-24-million-pay-off-voters-2024-10-24/

Turing Institute / CETaS. (2024). *AI-enabled influence operations: Safeguarding future elections.* https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-safeguarding-future-elections

Uribe Burcher, C. (2017). Assessing the threat of nexus between organized crime and democratic politics: Mapping the factors. *International Relations and Diplomacy*, 5(1). https://www.davidpublisher.com/index.php/Home/Article/index?id=30183.html

Uribe Burcher, C. (2019). *Cryptocurrencies and political finance.* International IDEA. https://www.idea.int/publications/catalogue/cryptocurrencies-and-political-finance

U.S. Cyber Command. (2024, September 12). Russian disinformation campaign Doppelgänger unmasked: A web of deception. https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/

U.S. Department of Justice (DOJ). (2024a). Election threats. https://www.justice.gov/archives/voting/election-threats

U.S. Department of Justice (DOJ). (2024b, September 4). Justice Department disrupts covert Russian government–sponsored foreign malign influence operation. https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

U.S. Office of the Director of National Intelligence (ODNI). (2024, March 11). *Annual threat assessment of the U.S. Intelligence Community.* https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

U.S. Office of the Director of National Intelligence (ODNI). (2025, March 18). *Annual threat assessment of the U.S. Intelligence Community 2025.* https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf

U.S. Treasury (OFAC). (2024a, September 4). Treasury takes action as part of a U.S. Government response to Russia's foreign malign influence operations. https://home.treasury.gov/news/press-releases/jy2559

U.S. Treasury (OFAC). (2024b, December 31). Treasury sanctions entities in Iran and Russia that attempted to interfere in the U.S. 2024 election. https://home.treasury.gov/news/press-releases/jy2766

V-Dem Institute. (2024). *Democracy report 2024: Democracy winning and losing at the ballot.* https://v-dem.net/publications/democracy-reports/

V-Dem Institute. (2025). *Autocratization turns viral: Democracy report 2025.* https://v-dem.net/publications/democracy-reports/

Vanderlee, K., & Collier, J. (2024, April 25). Poll vaulting: Cyber threats to global elections. *Google Cloud / Mandiant.* https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-global-elections

Weatherbed, J. (2024, November 14). Google says it will stop serving political ads in the EU. *The Verge:* https://www.theverge.com/2024/11/14/24296510/google-dropping-political-ads-in-the-eu-ttpa

Westminster Foundation for Democracy (WFD). (2025). *Understanding and addressing the cost of politics.* https://www.wfd.org/cost-of-politics

WHAS11. (2025, July 8). Jefferson County Clerk's Office says voting system remains safe after ransomware attack. https://www.youtube.com/watch?v=diY7hpMlY50

Wilson, A. (2023). *Democracy under siege: Tackling Russian interference in Moldova.* ECFR. https://ecfr.eu/article/democracy-under-siege-tackling-russian-interference-in-moldova/

Wilson Center. (2025, March 19). Ukraine's presidential elections amid war: Political, legal, and security challenges. https://www.wilsoncenter.org/blog-post/ukraines-presidential-elections-amid-war-political-legal-and-security-challenges

08 Ծանոթագրություններ

1 Global Witness, 2025; Meaker, 2023; Rainsford, 2024; McGrath & Alexandru, 2025
2 Bay et al., 2022; Hollis & Ohlin, 2021
3 Bay, 2024; EEAS, 2025a
4 Bay et al., 2022; Bay 2024; Levin, 2020; Ohlin, 2020
5 Pamment & Tsurtsumia, 2025
6 Տե՛ս Կանադայի Հեռահաղորդակցային Անվտանգության Կենտրոն, 2025; Must, 2025; ԱՄՆ Ազգային ռազմավարական վարչության տնօրենի գրասենյակ, 2025։
7 Bay, 2024
8 Stockwell et al., 2024; Csernatoni, 2024; Schroeder et al., 2025
9 Stockwell et al., 2024; Csernatoni, 2024; Schroeder et al., 2025
10 Bay, 2024; Hybrid CoE, 2025
11 Bay, 2024
12 Bay, 2024; Alihodžić, 2023; Center for an Informed Public et al., 2021
13 International IDEA, 2024
14 Bryjka, 2024; OSCE/ODIHR, 2025b; OSCE/ODIHR, 2025c
15 Gilbert, 2024
16 Center for an Informed Public et al., 2021
17 Center for an Informed Public et al., 2021; International IDEA, 2024; DFRLab, 2023; EUvsDisinfo 2024
18 Huo, 2024; Hedling, 2025
19 Hedling, 2025
20 Hoogensen Gjørv & Jalonen, 2023
21 Hedling, 2025
22 Hedling, 2025
23 ԱՄՆ Ազգային հետախուզության տնօրենի գրասենյակ, 2025թ.
24 Pamment & Tsurtsumia, 2025
25 Bay, 2024; Pamment & Isaksson, 2024; Pamment & Tsurtsumia, 2025
26 Hoffman, 2022
27 Atlantic Council 2023; Pamment & Tsurtsumia, 2025
28 Bay, 2024; European Commission, 2016; EEAS, 2024; EEAS 2025a; NATO, 2022; NATO, 2025
29 EEAS, 2025a; EEAS, 2025b
30 Տե՛ս Huo, 2024; Pamment & Tsurtsumia, 2025; Stockwell et al., 2024
31 Pamment & Tsurtsumia, 2025; Microsoft Threat Analysis Center, 2024a; Microsoft Threat Analysis Center, 2024b
32 EEAS, 2025a; U.S. Cyber Command, 2024
33 Pamment & Tsurtsumia, 2025
34 EDMO, 2024
35 Pamment & Tsurtsumia, 2025
36 EUvsDisinfo, 2024a
37 Bjola, 2025; IFES, 2024; Global Witness, 2024
38 Chan 2024; European Commission, 2024
39 Clayton, 2014; Atlantic Council, 2018
40 Nardelli, 2025
41 OSCE/ODIHR, 2024; OSCE/ODIHR, 2025b

42 Kubica, 2024; EUvsDisinfo, 2024b
43 Tanas, 2024; Balmforth & Dysa, 2024
44 Antoniuk, 2024; Antoniuk, 2025; Olari, 2024; Olari, 2025a; Olari, 2025b
45 Kubica, 2024; EUvsDisinfo, 2024a; DFRLab, 2024
46 Tanas, 2024; Balmforth & Dysa 2024; OSCE/ODIHR 2025; RFE/RL Moldovan Service, 2024
47 DFRLab, 2024; EUvsDisinfo, 2024a; Balmforth & Dysa, 2024
48 McGrath, 2025; IGP, 2025
49 McGrath, 2025; IGP, 2025
50 Moldpres, 2025; IGP, 2025
51 Antoniuk, 2023; Antoniuk, 2024; Antoniuk, 2025; Martin; 2022; OSCE/ODIHR, 2021
52 Cerulus, 2025; EEAS 2025c; European Commission 2025c
53 Pamment & Tsurtsumia, 2025
54 Euromaidan Press, 2014; EEAS, 2025a
55 Hedenskog & Hjelm, 2020; Lopatka, 2024
56 Clayton, 2014; Atlantic Council, 2018; Euromaidan Press, 2014
57 ODNI, 2024; ODNI, 2025
58 FBI, 2024; Reuters, 2024a; Roth, 2024; U.S. Treasury, 2024a, 2024b
59 DOJ, 2024b; Microsoft Threat Analysis Center, 2024b; Nakamura, Belton & Sommer, 2024
60 Atlantic Council, 2024; Microsoft Threat Analysis Center, 2024a; Reuters, 2024a
61 Bing & Vicens, 2024; DOJ, 2024a Gavin, 2025
62 DOJ, 2024a; FBI, 2024; U.S. Treasury, 2024a; 2024b
63 Kovalčíková & Spatafora, 2024; National Task Force on Election Crises, 2025a; National Task Force on Election Crises, 2025b; Turing CETaS, 2024
64 Bay, 2024
65 Ledford, 2024
66 Pamment & Tsurtsumia, 2025
67 Zuboff, 2019
68 Տե՛ս Mutu, 2024; Newman, Fletcher, Robertson, Ross Arguedas, & Nielsen, 2024
69 Եվրոպական հանձնաժողով, 2024թ.
70 Weatherbed, 2024; Chan, 2025
71 Elliott, 2024
72 O'Brien & Swenson, 2024; Brennan Center for Justice, 2024
73 C2PA, 2024
74 Google DeepMind, 2025
75 Newman et al., 2024
76 Pamment & Tsurtsumia, 2025
77 Bateman & Jackson, 2024; Bay, 2025; Pamment et al. 2018; Pamment & Isaksson, 2024
78 OECD 2021; OECD 2022
79 ENISA 2023; International IDEA 2023; Bay 2025
80 Center for an Informed Public et al. 2021
81 Lewandowsky et al., 2020
82 EEAS, 2025
83 OECD, 2021
84 Center for an Informed Public et al., 2021; C2PA, 2024; ENISA, 2023
85 OECD, 2022
86 C2PA, 2024; Google DeepMind, 2025
87 Perdomo & Uribe Burcher, 2017: 128; WFD, 2025
88 Bakken, 2025; Popescu-Zamfir, 2025; OSCE/ODIHR, 2017: 12; 2021: 16
89 International IDEA, 2025
90 OSCE/ODIHR, 2025a: 1–2
91 Wilson, 2023
92 Wilson, 2023; OSCE/ODIHR, 2025b: 1
93 International IDEA, 2025
94 Perdomo & Uribe Burcher, 2017: 134
95 CoinGecko, 2025; Lores, 2025; Chainalysis, 2024a
96 Coherent Market Insights, 2025
97 Uribe Burcher, 2019: 14

98 Uribe Burcher, 2019: 13; Chainalysis, 2024b
99 International IDEA, 2025
100 Perdomo & Uribe Burcher, 2017: 139; Wolfs, 2025: 3–4
101 Wolfs, 2025: 5
102 Agrawal, Hamada & Fernández Gibaja, 2021: 12
103 Ryan, 2018; Britzky, 2018
104 DOJ, 2024a
105 IFES, 2024
106 OSCE/ODIHR, 2025a: 8–9
107 Perdomo & Uribe Burcher, 2017: 137–138
108 Եվրոպայի խորհուրդ, 2025թ. 4
109 International IDEA, 2025
110 Wolfs, 2025: 2
111 Perdomo & Uribe Burcher, 2017: 141
112 Uribe Burcher, 2019: 7, 9–11
113 Vasani, James & Holly, 2022
114 Uribe Burcher, 2019: 15–16
115 International IDEA, 2025
116 Perdomo & Uribe Burcher, 2017: 138–139
117 Uribe Burcher, 2019: 16
118 Wolfs, 2025: 2
119 Perdomo & Uribe Burcher, 2017: 144
120 International IDEA, 2025
121 V-Dem, 2024; V-Dem, 2025; UNESCO, 2025; Posetti et al., 2020
122 Council of Europe, 2025; Liberties, 2025; Freedom House, 2024
123 CIVICUS, 2024; OSCE/ODIHR, 2023
124 OECD, 2021; OSCE/ODIHR, 2023
125 Perdomo & Uribe Burcher, 2017: 136
126 Europol, 2025a; Hoxhunt, 2025
127 Bay, 2024
128 Uribe Burcher, 2017
129 Europol, 2025a
130 Cyble, 2024
131 Deloitte, 2024
132 Europol, 2025a
133 Europol 2025a; Deloitte 2024
134 Must, 2025; ReliaQuest, 2024
135 ReliaQuest, 2024; Center for Internet Security, 2025a
136 Europol, 2025a
137 CISA, 2024
138 CISA, 2024
139 Hoxhunt, 2025
140 Forbes 2025
141 CISA 2024a; NIST 2020; FIDO Alliance 2023; ENISA 2023; MS-ISAC 2024; C2PA 2024
142 Bay, 2024; ReliaQuest, 2024
143 Bay et al., 2022
144 Bay, 2024
145 UK Electoral Commission, 2024
146 Euromaidan Press, 2014
147 Alliance for Securing Democracy, 2019
148 Council of Europe, 2024; Wilson Center, 2025
149 CNN, 2024a
150 WHAS11, 2025
151 Constella Intelligence, 2025
152 Ինտերնետային անվտանգության կենտրոն, 2025a, Ինտերնետային անվտանգության կենտրոն, 2025b, Ինտերնետային անվտանգության կենտրոն, 2025c
153 Cloudflare, 2025

154 Saeva & Tasheva, 2024
155 Bay et al., 2022; County of San Luis Obispo, 2024
156 Bay, 2024; ReliaQuest, 2024
157 Electionline, 2024
158 Ivanti, 2025
159 Cyble, 2025
160 ReversingLabs 2025; ISACA, 2025 թ
161 ISACA, 2025
162 Cisco, 2025
163 International IDEA, 2019
164 Bay, 2024
165 Google Cloud, 2023
166 CISA, 2024
167 Molas, 2024; Cybersecurity Dive, 2024
168 Stimson Center, 2024
169 International IDEA 2019; Bay 2024; Google Cloud 2023; CISA 2024a; Stimson Center 2024
170 Տե՛ս Microsoft, 2025
171 Vanderlee & Collier, 2024; NCSC, 2025
172 Bay, 2024; International IDEA, 2023
173 Center for Internet Security 2025a; NIST, 2022; NIST, 2024
174 CrowdStrike 2025a; NIST, 2020; NIST, 2023
175 CISA, 2024b; CrowdStrike, 2025b
176 CISA & EAC, 2024a; CISA & EAC, 2024b; CISA, 2024b
177 Bay, 2024; Bay, 2025
178 Bay, 2024
179 Canada, 2025
180 Bay, 2024
181 Bay, 2024
182 Եվրոպական հանձնաժողով, 2016; Եվրոպական հանձնաժողով, 2025b
183 Bay, 2024; Bay, 2025
184 Bay, 2025
185 GAO, 2020
186 Columbia University, 2025
187 Կանադայի ընտրություններ, 2025
188 Կանադայի կառավարություն, 2025; PCO, 2025
189 Կանադա, 2025, CISA 2025
190 Տե՛ս Bay, 2025
191 Hybrid CoE, 2024
192 Bay, 2025; Canada, 2025
193 Եվրոպական հանձնաժողով, 2025b
194 Bay, 2024; Elections Canada, 2025
195 Եվրոպական հանձնաժողով, 2025b
196 Եվրոպական հանձնաժողով, 2025a
197 NATO, 2024; Elections Canada, 2025
198 International IDEA, 2025; The Carter Center, 2025
199 US Office of the Director of National Intelligence, 2025; Pamment & Tsurtsumia, 2025
200 Pamment & Tsurtsumia, 2025
201 Stockwell et al. 2024; CISA, 2024a
202 IFES 2024; Bay, 2024
203 Brennan Center for Justice, 2020; Elliott, 2024; European Commission, 2024; C2PA, 2024; Pamment & Tsurtsumia, 2025

Ֆոլկե Բերնադոտի ակադեմիան (ՖԲԱ) Շվեդիայի կառավարության խաղաղության, անվտանգության և զարգացման գործակալությունն է: Որպես Շվեդիայի միջազգային զարգացման համագործակցության մաս, մենք խթանում ենք խաղաղությունը հակամարտություններից տուժած երկրներում: Մենք առաջարկում ենք վերապատրաստում և խորհրդատվություն, ինչպես նաև անցկացնում ենք հետազոտություններ՝ խաղաղության և անվտանգության համատեքստում խաղաղության կառուցումն ու կառավարումը ամրապնդելու համար: Ավելին, մենք քաղաքացիական անձնակազմեր ենք տեղակայում խաղաղապահ գործողություններում և ընտրությունների դիտորդական առաքելություններում, որոնք հիմնականում ղեկավարվում են ՄԱԿ-ի, ԵՄ-ի և ԵԱՀԿ-ի կողմից: Գործակալությունը անվանակոչվել է ՄԱԿ-ի առաջին խաղաղության միջնորդ, կոմս Ֆոլկե Բեռնադոտի անունով:

Եթե ցանկանում եք ավելին իմանալ ՖԲԱ-ի մասին, հետևեք մեզ հետևյալ կայքերում

linkedIn.com/FolkeBernadotteAcademy

instagram.com/FolkeBernadotteAcademy

facebook com/FolkeBernadotteAcademy

soundcloud.com/FolkeBernadotteAcademy

www.fba.se

Ֆոլկե Բեռնադոտ ակադեմիա
Խաղաղության, անվտանգության և զարգացման շվեդական գործակալություն

FBA