ՔԱՂԱՔԱԿԱՆՈՒԹՅԱՆ ՀԵՏԱԶՈՏԱԿԱՆ ԿԵՆՏՐՈՆ

CENTRE FOR POLICY STUDIES

Visegrad Fund

Ministry of Foreign Affairs
Republic of Korea

Արմեն Գրիգորյան

Armen Grigoryan

Կիբեռանվտանգության ոլորտում Վիշեգրադյան քառյակի երկրների քաղաքականության որոշ առանձնահատկություններ

Some characteristics of the Visegrad Four states' cybersecurity policies

Ծրագիրն իրականացվել է գործընկերների մասնակցությամբ.

«Res Publica» հիմնադրամ (Լեհաստան)
Բուդապեշտի հանրային քաղաքականության վերլուծությունների ինստիտուտ (Հունգարիա)
Քաղաքականության և հասարակության ինստիտուտ (Չեխիա)
«Ռազմավարական վերլուծություն» կենտրոն (Սլովակիա)

The project was implemented in cooperation with

Institute for Politics and Society (Czech Republic)
Budapest Institute for Policy Analysis (Hungary)
Res Publica Foundation (Poland)
Strategic Analysis Think Tank (Slovakia)

Սույն հրապարակումը լույս է տեսնում Քաղաքականության հետազոտական կենտրոնի կողմից Միջազգային Վիշեգրադյան հիմնադրամի և Կորեայի Հանրապետության ԱԳՆ-ի օժանդակությամբ իրականացված «Վիշեգրադյան քառյակի փորձի կիրառումը Հայաստանում խորացված բարեփոխումների համար» ծրագրի շրջանակում:

Ծրագիրը ֆինանսավորվում է Լեհաստանի, Հունգարիայի, Չեխիայի և Սլովակիայի կառավարությունների կողմից՝ Միջազգային Վիշեգրադյան հիմնադրամի միջոցով, որի նպատակը Կենտրոնական Եվրոպայում հարատև տարածաշրջանային համագործակցության առաջխաղացումն է:

This paper is published within the framework of the *Further Support for Reforms in Armenia with Visegrad Four's Know-how* project funded by the International Visegrad Fund and the Ministry of Foreign Affairs of the Republic of Korea.

The project is co-financed by the Governments of Czechia, Hungary, Poland and Slovakia through Visegrad Grants from International Visegrad Fund. The mission of the fund is to advance ideas for sustainable regional cooperation in Central Europe.

Grant #22220233

Լրացուցիչ մանրամասներ առկա են https://centreforpolicystudies.org/pr6.html էջում
Additional information: https://centreforpolicystudies.org/en-pr6.html

Հոդվածաշարի խմբագիր՝ **Արմեն Գրիգորյան**
Series editor: **Armen Grigoryan**

Երևան 2023
Yerevan, 2023

Արմեն Գրիգորյան

Կիբերանվտանգության ոլորտում Վիշեգրադյան քառյակի երկրների քաղաքականության որոշ առանձնահատկություններ

«Կիբերանվտանգություն» եզրույթն առնչվում է ժամանակակից տեխնոլոգիաների հետ կապակցված գրեթե բոլոր երևույթներին: Ներկայիս թվային ժամանակաշրջանում մեր կյանքը բազմաթիվ առումներով սերտորեն կապված է համացանցի, համակարգիչների, այլ սարքավորումների և համակարգչային ծրագրերի հետ: Կենսական նշանակության բոլոր ենթակառուցվածքները՝ բանկային համակարգը, էլեկտրական ցանցերը, առողջապահությունը, օդային հաղորդակցությունը և այլն, ինչպես նաև պետական հիմնարկները, արտադրական ձեռնարկությունների բնականոն աշխատանքը կապված է համացանցի հետ: Անհատները նույնպես զգալիորեն կախված են մշտապես համացանցին միացրած սարքավորումներից՝ կատարելով գնումներ, օգտվելով սոցիալական ցանցերից, առցանց քարտեզներից, խաղերից և բազմաթիվ այլ ծառայություններից:

Տեխնոլոգիաները գնալով ավելի ու ավելի են զարգանում. նույնը տեղի է ունենում կիբերհարձակումների հետ: Համընդհանուր փոխկապակցվածությունը և տվյալների առցանց շտեմարանների օգտագործումը հանգեցնում են թե՛ անմիջական, թե՛ երկրորդական ռիսկերի ավելացմանը: Համակարգերի փոխկապակցվածությունը և տեխնիկական բարդությունը, որին է՛լ ավելի են նպաստելու նորաստեղծ տեխնոլոգիաները՝ 5G ցանցերը, արհեստական բանականությունը, քվանտային տեխնոլոգիաները և այլն, հետագայում կարող են հանգեցնել առավել մեծ փոխկապակցված վտանգների: Որոշ համակարգերի սեփականատերեր նույնպես կարող են նպաստել տվյալների անվտանգության և կենսական ենթակառուցվածքների համար առկա սպառնալիքներին:

Տարբեր տեսակի տվյալներ՝ անձնական տվյալները, մտավոր սեփականությունը, ֆինանսական տվյալները և այլն, կարող են վտանգվել դրանց արտահոսքի և ապօրինի օգտագործման պատճառով՝ ինչը հղի է զանազան բացասական հետևանքներով: Հանցագործները, թշնամական պետությունները և պարզապես տարատեսակ անբարեխիղճ օգտատերեր կարող են ձեռք բերված տվյալներն օգտագործել նյութական շահ հետապնդելու, դրամաշորթության, քաղաքական նպատակներ իրականացնելու և այլ նպատակներով. այդպիսով, տվյալների արտահոսքը հղի է լուրջ վտանգներով՝ անձնական կյանքի, տնտեսության և ազգային անվտանգության համար: Հետևաբար, կիբերանվտանգությունը հատկապես կարևոր է բոլոր տեսակի տվյալները պահպանելու համար՝ ցանցերը և սարքավորումները արտաքին միջամտությունից պաշտպանող սարքերի և գործիքակազմի միջոցով: Այն կարող է օգնել տվյալների արտահոսքերը, ինքնության յուրացումը և այլ կիբերհանցագործությունները կանխելուն:

Կիբերանվտանգությունը կարող է բաժանվել մի քանի ենթատիրույթների.

- Ցանցային անվտանգությունը ներառում է համակարգչային ցանցերի պաշտպանությունը ապօրինի ներխուժումներից, խափանումներից և ոչ նպատակային օգտագործումից՝ սարքավորումների և ծրագրային ապահովման միջոցով,
- Ծրագրային անվտանգությունը կապված է ծրագրերի և սարքավորումների պաշտպանության հետ: Այն հնարավոր է դառնում ծրագրերի թարմացման միջոցով՝ առավել ապահովության համար: Անվտանգությունը պետք է

ապահովվի նաև ծրագրային ապահովման ստեղծման բոլոր փուլերում՝ ծրագրային կոդը գրելու, վավերացման, սպառնալիքների մոդելավորման և այլն,

- Տեղեկատվական կամ տվյալների անվտանգությունը կապված է տվյալների կրիչների և փոխանցման ուղիների պաշտպանության հետ՝ գաղտնիության պահպանման համար,
- Ինքնությունների կառավարումը անհատների և այլ օգտատերերի համար թույլատրելի հասանելիության մակարդակի որոշումն է,
- Գործառնական անվտանգությունը տվյալների ռեսուրսները կառավարելու և դրանց անվտանգությունն ապահովելու մասին որոշումների կայացման գործընթացն է,
- Շարժական սարքերի անվտանգությունը կապված է բջջային հեռախոսներում, շարժական համակարգիչներում, պլանշետներում և այլ սարքերում պահվող անձնական և այլ տվյալների պաշտպանության հետ՝ դրանք ապօրինի օգտագործումից, սարքերի կորստից կամ գողությունից, համակարգչային վիրուսներից և այլ վտանգներից ապահովելու համար,
- Առցանց շտեմարանների անվտանգությունը դրանցում պահպանվող տվյալների պաշտպանությունն է,
- Վթարների վերացումը և շարունակականության պլանավորումը տվյալների կորստով կամ աշխատանքի խափանմամբ հղի ապօրինի միջամտություններին հակազդելու գործիքակազմն է՝ մշտադիտարկումը, կանխազգուշացման համակարգը, գործողությունների պլանները:[1]

Կիբերանվտանգության համար առանցքային նշանակություն ունի նաև օգտատերերի ուսուցումը: Սպառնալիքների մասին տեղեկացվածությունը, անվտանգության միջոցների մասին տեղեկացվածությունը, կարգադրությունների և պահանջների կատարումը կարող են նվազեցնել կիբերհանցագործությունների զոհ դառնալու վտանգը՝ թե անհատների, թե կազմակերպությունների համար:

2020 թ. ընդունված ՀՀ Ազգային անվտանգության ռազմավարությունը ներառում է «Բաց և անվտանգ տեղեկատվական և կիբերտիրույթների ապահովում» հակիրճ ենթագլուխը, որում մասնավորապես նշված է.

> «Հայաստանի տեղեկատվական անվտանգությանը սպառնում են օտարերկրյա պետությունների, միջազգային ահաբեկչական կազմակերպությունների, հանցավոր խմբավորումների և անհատների կողմից Հայաստանի տարածքում գտնվող տեղեկատվական ռեսուրսների նկատմամբ կիբերհարձակումները: ... Ժամանակակից աշխարհում ավելի սուր դրսևորումներ են ստանում տեղեկատվական պատերազմները, որոնք ներառում են քարոզչության, մանիպուլյացիաների, կեղծ լուրերի և ապատեղեկատվության գործիքակազմ և հաճախ թիրախավորում են ժողովրդավարական արժեքները: Այս համատեքստում մենք աշխատելու ենք հանրային իրազեկվածության և մեդիագրագիտության մակարդակի բարձրացման ուղղությամբ՝ նպատակ ունենալով հզորացնել տեղեկատվական պատերազմներին հակազդելու հասարակության և պետության կարողությունները: ... Առաջնային մարտահրավերներից է տեղեկատվական և կիբերանվտանգության ոլորտը կարգավորող

[1] 'What is Cyber Security?' https://www.javatpoint.com/what-is-cyber-security.

> համապարփակ պետական քաղաքականության անկատարությունը, կենսական նշանակության տեղեկատվական ենթակառուցվածքների պաշտպանությունն ապահովող օրենսդրության բացակայությունը, համակարգչային պատահարների արձագանքման կառույցների ինստիտուցիոնալ կարողությունների ոչ բավարար մակարդակը և կիբերանվտանգության ոլորտը համակարգող կառույցի բացակայությունը: ... Տեղեկատվական տիրույթում դիմակայունությունը բարձրացնելու համար մենք զարգացնելու ենք ազգային տեղեկատվական և կիբեր կարողությունները՝ ռիսկերի արդյունավետ կառավարման, որակավորված մասնագիտական ներուժի ձևավորման, միջազգային ստանդարտների տեղայնացված ներդրման, թվային գրագիտության մակարդակի բարձրացման միջոցով»:[2]

Ռազմավարությունում կիրառվող ձևակերպումների առումով առկա է առաջընթաց՝ 2007 թ. ընդունված նախորդ ռազմավարության համեմատ: Այնուամենայնիվ, գործնական առաջընթացն առայժմ սահմանափակ է: Թվային և տեղեկատվական անվտանգության համապարփակ ռազմավարություն դեռևս առկա չէ. դա մասնավորապես նկատելի է կիբերհարձակումների ժամանակ:

Միևնույն ժամանակ, ոլորտի համար պատասխանատու կառավարական մարմինները պատրաստ են համագործակցելու հնարավոր գործընկերների հետ: Բարձր տեխնոլոգիական արդյունաբերության նախարարությունը, բացի օրենսդրության և քաղաքականության իրականացման բարելավման նպատակով օտարերկրյա գործընկերների հետ համագործակցության հնարավորությունները քննարկելու պատրաստակամությունից, նաև օժանդակում է օգտատերերի ուսուցմանը: Այսպես՝ վերջերս Տեղեկատվական և հաղորդակցության տեխնոլոգիաների գործատուների միության հետ համագործակցությամբ կազմակերպվել էր դասընթաց, որի արժեքի 30-80% մասնակիցների համար սուբսիդավորվել էր կառավարության կողմից:[3]

Սույն հոդվածում ամփոփված են Քաղաքականության հետազոտական կենտրոնի կողմից Միջազգային վիշեգրադյան հիմնադրամի և Կորեայի Հանրապետության ԱԳՆ-ի օժանդակությամբ իրականացված ծրագրի որոշ արդյունքներ: Մասնավորապես, հոդվածը կենտրոնանում է ծրագրին մասնակցած փորձագետների պրեզենտացիաների որոշ հատվածների վրա՝ նաև ներկայացնելով լրացուցիչ տեղեկություններ, որոնք կարող են նպաստել Հայաստանի կիբերանվտանգության քաղաքականության մշակումն ու իրականացումը բարելավելուն:

Ազգային անվտանգության ռազմավարությունների և քաղաքականությունների համեմատություն

Վիշեգրադյան քառյակի երկրների ազգային անվտանգության ռազմավարությունների և դրանցից բխող քաղաքականությունների միջև նշանակալի նմանություններ կան՝ ինչը պայմանավորված է նրանց ՆԱՏՕ-ի և ԵՄ-ի անդամի կարգավիճակով. քաղաքականության առանցքային տարրերի

[2] ՀՀ Ազգային անվտանգության ռազմավարություն, էջ 30-31, https://www.primeminister.am/u_files/file/Different/AA-Razmavarutyun-Final.pdf
[3] https://edu.hti.am/trainings/cybersecurity

համապատասխանեցումը ՆԱՏՕ-ի, ԵՄ-ի և դաշնակից պետությունների նկատմամբ ստանձնած պարտավորությունների մասն է:

2018 թ. Եվրոպական խորհրդարանը, ԵՄ Խորհուրդը և Եվրոպական հանձնաժողովը հասել են կիբերանվտանգության մասին օրենքի վերաբերյալ քաղաքական համաձայնության՝ վերահաստատելով ԵՄ-ի Կիբերանվտանգության գործակալության լիազորությունները՝ կիբերանվտանգության սպառնալիքներին և կիբերհարձակումներին առավել արդյունավետորեն դիմակայելու նպատակով անդամ պետություններին օգնելու համար: Օրենքով սահմանվել է կիբերանվտանգության ոլորտում սերտիֆիկացման ընդհանուր ընթացակարգը՝ ներառյալ առցանց ծառայությունների և օգտատերերի կողմից կիրառվող սարքերի անվտանգության ապահովումը: Հատկանշական է սակայն, որ վերջինիս առումով նշվել է. «Քանի դեռ ԵՄ-ի քաղաքացիների առօրյա կյանքի բոլոր ասպարեզներում առկա են օտարերկրյա արտադրության սարքեր և ծրագրային ապահովում, անվտանգությունը կմնա անհասանելի երազանք»:[4]

Չնայած ՆԱՏՕ-ի և ԵՄ-ի անդամներին հասանելի ընդլայնված հնարավորություններին, կիբերանվտանգության ոլորտում Վիշեգրադյան քառյակի երկրները մեծապես դիմակայում են նույն մարտահրավերներին՝ ինչպես Հայաստանը: Դրանով է պայմանավորված որոշ ձևակերպումների համընկնումը և որոշ լուծումների նմանությունները՝ գոնե տեսականորեն: Միևնույն ժամանակ, արժե ուշադրություն դարձնել հատկապես քաղաքականության որոշ նորագույն ասպեկտների, ինչպես նաև որոշ պետական մարմինների կառուցվածքին՝ որպես դրական օրինակներ:

Չեխիա

Համակարգչային արտակարգ իրավիճակների արձագանքման թիմը (CERT) գործում է 2011-ից որպես CSIRT.CZ (CSIRT՝ Cyber Security Incident Response Team, Կիբերանվտանգության միջադեպերի արձագանքման թիմ). Դրա իրավասությունները սահմանվում են 2014 թ. թիվ 181/2014 օրենքով (կիբերանվտանգության մասին օրենք) և Կիբեր և տեղեկատվական անվտանգության ազգային գործակալության (NÚKIB) հետ կնքված պայմանագրով: NÚKIB-ը կիբերանվտանգության ոլորտի կենտրոնական վարչական մարմինն է, որը պատասխանատու է տեղեկատվական և հաղորդակցության համակարգերում տեղեկատվության գաղտնիության, կրիպտոգրաֆիայի, ինչպես նաև «Գալիլեո» արբանյակային համակարգի հետ փոխկապակցված ոչ հանրային բնույթի ծառայությունների համար:[5] Այն նաև իր կայքի միջոցով պարբերաբար հրապարակում է նախազգուշացումներ առկա վտանգների մասին և խորհրդատվություն է տրամադրում:

2015 թ. ընդունված Չեխիայի Հանրապետության անվտանգության ռազմավարությունը սահմանում է, որ հանրային և մասնավոր հատվածների դեմ ուղղված կիբերհարձակումների հայտնի ռիսկերից, առկա են լրացուցիչ ռիսկեր

[4] Botond Feledy, 'Cyber security and Sovereignty: Two levels of digital autonomy'. Think Visegrad policy brief, 2018, https://europeum.org/en/articles/detail/2454/cyber-security-and-sovereignty-two-levels-of-digital-autonomy.

[5] National Cyber Security Strategy of the Czech Republic, p. 7, available at https://nukib.cz/en/cyber-security/strategy-action-plan/.

կենսական ենթակառուցվածքների համար, և վերջիններիս պաշտպանությունը ներառում է այդ ոլորտներում և ռազմավարական ձեռնարկություններում օտարերկրյա ներդրումների մշտադիտարկումը՝ նման ներդրումներն օտար պետությունների կողմից իրենց շահերի առաջխաղացման համար օգտագործելու հնարավորությունները բացառելու համար: Դա մասնավորապես վերաբերվում է էներգետիկ և տեղեկատվական ու հաղորդակցության տեխնոլոգիաներին:[6]

2016-ին իրականացված ազգային անվտագության աուդիտը հիմնված էր համապարփակ ռազմավարական վերլուծության վրա՝ չեխ հասարակությանը համար սպառնալիքների և ազգային անվտանգության թույլ կողմերի գնահատմամբ: Ըստ աուդիտի բնորոշման, ազգային անվտանգության համար հիմնական սպառնալիքները բաժանվում են հինգ տեսակի՝ կիբեր լրտեսություն, տեղեկատվական տեխնոլոգիաների հետ կապված ենթակառուցվածքի խափանումը կամ դիմակայունության թուլացումը, թշնամական քարոզչությունը, հանրային ծառայությունների խափանումը կամ անվտանգության մակարդակի նվազումը, ինչպես նաև կիբեր ահաբեկչությունը:

Ըստ սպառնալիքների մակարդակի գնահատման, Չեխիայում բարձր է կիբեր լրտեսության հավանականությունը՝ գաղտնի, ռազմավարական նշանակություն ունեցող, ինչպես նաև անձնական տվյալներ ստանալու նպատակով, ու նաև բարձր է տեղեկատվական տեխնոլոգիաների հետ կապված ենթակառուցվածքի խափանումը կամ դիմակայունության թուլացումը: Վերջինիս հետ կապված ռիսկերը և մարտահրավերները մասամբ կապված են պետական ծառայողների՝ կիբերանվտանգության ոլորտում գիտելիքների պակասի և «թվային հիգիենայի»[7] կանոններին չհետևելու հետ, ինչպես նաև որոշ նախարարությունների և այլ կառույցների կողմից ծախսերը պլանավորելիս կիբերանվտանգության տեխնոլոգիաները և այլ թվային գործիքները որպես առաջնահերթություն չդիտարկելը: Միևնույն ժամանակ, կիբեր ահաբեկչության և հանրային ծառայությունների խափանման կամ անվտանգության մակարդակի նվազման վտանգները գնահատվում են միջին մակարդակի. վերջինիս դեպքում, ռիսկի գործոններից են կիբերանվտանգության քաղաքականության վատ պլանավորումը, ինչպես նաև դարձյալ՝ պետական ծառայողների անուշադրությունը:[8]

Մեկ այլ մասնագիտացված և վերջերս վերանայված փաստաթուղթ էլ 2021-2025 թթ. Կիբերանվտանգության ազգային ռազմավարությունն է՝ հիմնված հասարակությանը սպառնացող հիմնական վտանգների և ազգային անվտանգության համակարգում թերությունների ու բացթողումների համապարփակ ռազմավարական վերլուծության վրա: Դրանում մասնավորապես նշված է տեղեկատվական հասարակության անցման հետ կապված խնդիրների առկայությունը՝ ներառյալ թվային հիգիենայի, մեդիագրագիտության և քննադատական մտածողության պակասը: Նշվում է, որ պետությունը պետք է կրթական համակարգի բոլոր մակարդակներում ներառի կիբերանվտանգությունը՝ որպես ցանկացած ոլորտի առնչվող խնդիր, հատկապես շեշտելով անվտանգության

[6] Security Strategy of the Czech Republic, https://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf, p. 20.

[7] «Թվային հիգիենան» բնութագրվում է որպես կանոնների, գործընթացների և սովորությունների համադրություն, որն օգտատերերին թույլ է տալիս անվտանգ կերպով օգտվել կիբերտիրույթից՝ դրսևորելով պրոակտիվ վերաբերմունք թվային հետքերի, անվտանգության և այլ հանգամանքների նկատմամբ:

[8] National Security Audit, https://www.mvcr.cz/chh/soubor/national-security-audit.aspx, pp. 97–104.

կարևորությունը՝ ցանկացած էլեկտրոնային սարքավորում օգտագործելիս:[9] Ռազմավարությունը փոխլրացվում է գործողությունների պլանով, որում թվարկված են կիբերանվտանգության ոլորտում անհրաժեշտ գործողությունները, դրանց իրականացման համար պատասխանատու մարմինները, ինչպես նաև իրականացման ժամկետները:[10]

Քաղաքականության և հասարակության ինստիտուտի փորձագետ Յան Հավլիչեկը, ով Հայաստան էր եկել 2022 թ. դեկտեմբերին՝ Քաղաքականության հետազոտական կենտրոնի կազմակերպած ծրագրի շրջանակում, «Առավոտ» օրաթերթի հետ հարցազրույցում մասնավորապես նշել էր, որ 2022 թ. հուլիս-դեկտեմբեր ժամանակահատվածում Չեխիայի ԵՄ նախագահության կողմից կազմակերպվել է բարձրագույն մակարդակով համաժողով՝ կիբերանվտանգության և Եվրոպայի թվային ապագայի թեմայով, որին մասնակցեցին նաև ԱՄՆ-ի և Ավստրալիայի ներկայացուցիչները: Չեխիայի նախագահության ներքո ԵՄ անդամները նաև միասնական դիրքորոշում են համաձայնեցրել՝ Եվրոպական պառլամենտում քննարկվելիք ԵՄ կառույցներում կիբերանվտանգության բարելավման միջոցների վերաբերյալ: Նոյեմբերին ԵՄ Խորհուրդը, պառլամենտը և Եվրոպական հանձնաժողովը համաձայնեցրել են թվային տիրույթում եվրոպական արժեքները՝ մասնավորապես ժողովրդավարությունը, հավասարությունը և կայուն զարգացումը, պահպանելու և առաջ մղելու միջոցներ: Բացի այդ, Չեխիայի նախագահությունը նաև Եվրոպական պառլամենտի հետ հաջողությամբ բանակցել է արտադրանքի անվտանգության չափանիշների մասին:[11] Վերջինս ուղղակիորեն փոխկապակցված է վերը նշված՝ օտարերկրյա արտադրության սարքավորումների և ծրագրային ապահովման խնդրի հետ:

Բացի այդ, Չեխիան նաև նախապատրաստել էր Արևելյան գործընկերության երկրների դիմակայունության ուժեղացմանը նպատակաուղղված քաղաքականության առաջարկների փաթեթը, որում նշված էր նաև հիբրիդային սպառնալիքների, այդ թվում՝ կիբերհարձակումների դեմ պայքարելու համար, համագործակցության անհրաժեշտությունը: Դա մասնավորապես հիշատակվել էր այն ժամանակ Չեխիայի փոխդեսպանի պաշտոնը զբաղեցրած Յան Պլեշինգերի կողմից՝ Քաղաքականության հետազոտական կենտրոնի կողմից Միջազգային վիշեգրադյան հիմնադրամի օժանդակությամբ իրականացված նախորդ ծրագրի շրջանակում 2020 թ. հուլիսի 13-ին կազմակերպված «Արևելյան գործընկերություն. հայացք Չեխիայից» սեմինարի բացման խոսքում:[12]

Հունգարիա

Կիբերանվտանգության ոլորտում Հունգարիայի քաղաքականությունն այս ծրագրի շրջանակում հատուկ չի ուսումնասիրվել. հունգարացի փորձագետների հետ քննարկումները կենտրոնացել են այլ թեմաների վրա: Կարելի է սակայն նկատել, որ

[9] National Cyber Security Strategy of the Czech Republic, p. 18, available at https://nukib.cz/en/cyber-security/strategy-action-plan/.
[10] Action Plan for the National Cyber Security Strategy of the Czech Republic, available at https://nukib.cz/en/cyber-security/strategy-action-plan/.
[11] Էմմա Գաբրիելյան, «Հիբրիդային սպառնալիքները՝ ուշադրության կենտրոնում», «Առավոտ», 21.12.2022, https://www.aravot.am/2022/12/21/1312592/
[12] «Չեխիան շարունակելու է Հայաստանին սատարել ԱլԳ շրջանակներում», 1in.am, 14.07.2020, https://www.1in.am/2787790.html

2020 թ. Հունգարիայի ազգային անվտանգության ռազմավարությունը դիտարկում է կիբերտիրույթը որպես առանձին ոլորտ՝ ցամաքի, ծովի, օդային տարածքի և տիեզերքի կողքին, և ապագա հակամարտությունները կիբերտիրույթ տեղափոխելու հավանականությունը շատ բարձր է գնահատվում: Քանի որ թվային գործիքները կարող են սպառնալ ֆիզիկական անվտանգությանը կամ խոշոր նյութական վնաս հասցնել, ռազմավարությամբ պետությանն իրավունք է վերապահվում կիբերհարձակումներին պատասխանել կոնվենցիոնալ միջոցներով. միաժամանակ նշվում է, որ, հաշվի առնելով մեղավորներին հայտնաբերելու բարդությունը, պատասխան գործողություններից առաջ անհրաժեշտ է իրականացնել մանրազնին հետաքննություն:[13] Ընդհանուր առմամբ, սա ենթադրում է, որ որոշ դեպքերում կիբերհարձակումները կարող են դառնալ ՆԱՏՕ-ի դաշնակիցներին կազմակերպության կանոնադրության 5-րդ հոդվածի համապատասխան դիմելու անհրաժեշտություն:

Ռազմավարությամբ նաև կարևորվում է կիբերանվտանգության ոլորտում վիճակի բարելավումը՝ հիմնվելով Հունգարիայում կատարված հետազոտությունների վրա: Հաշվի առնելով, որ հունգարական համալսարաններից մի քանիսն առաջադիմել են կիրառական մաթեմատիկայի և այլ հարակից ոլորտներում, հնարավոր է աշխատել գիտական համագործակցության զարգացման ուղղությամբ: Մասնավորապես, կարելի է նման համագործակցության հնարավորությունը քննարկել դիվանագիտական հարաբերությունները վերականգնելուն զուգորդող բանակցությունների ընթացքում:

Լեհաստան

Լեհաստանի Հանրապետության ազգային անվտանգության ռազմավարությունն ընդունվել է 2020 թ.: Դրանով նախատեսվում է ուժեղացնել կիբերսպառնալիքների նկատմամբ դիմակայունությունը՝ հանրային կառավարման, ռազմական և մասնավոր ոլորտներում: Այդ նպատակով նախատեսվում է զարգացնել կարողությունները հետազոտական, փորձարկման, գնահատման և կիբերանվտանգության ծառայությունների սերտիֆիկացման ոլորտներում: Մասնավորապես, առաջարկվող միջոցներից են «ժամանակակից տեխնոլոգիաների ոլորտում հետազոտությունների պետական ֆինանսավորման միջոցով կիբերանվտանգությանն առնչվող սեփական լուծումների մշակումը՝ այդ թվում մեքենայական ուսուցման, իրերի ինտերնետի (IoT), լարային և շարժական ցանցերի (5G և հաջորդ սերունդների)՝ համալսարանների, գիտական հաստատությունների, և հանրային ու մասնավոր հիմնարկների հետ համագործակցությամբ»:[14] Ռազմավարությունում նաև նշված է, որ թվային տիրույթում պետության և քաղաքացիների անվտանգ գործունեությունն ապահովելու համար պետք է զարգացնել կարողությունները՝ միավորելով երեք

[13] Hungary's National Security Strategy. A Secure Hungary in a Volatile World. https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html#:~:text=83)%20Hungary%20regards%20its%20primary,human%20rights%20and%20fundamental%20freedoms.

[14] National Security Strategy of the Republic of Poland, p. 20, https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

շերտեր. վիրտուալը (օպերացիոն համակարգեր և ծրագրեր), ֆիզիկականը (ենթակառուցվածքներ և սարքավորումներ) և ընկալումները:[15]

Սրա առնչությամբ ծրագրի շրջանակում 2023 թ. հունվարին «Res Publica» հիմնադրամի նախագահ, «Visegrad Insight» հանդեսի գլխավոր խմբագիր Վոյչեխ Պշիբիլսկու Երևան կատարած այցի ընթացքում տեղի ունեցած «Լեհաստանի անվտանգային քաղաքականությունը» թեմայով համաժողովում մասնավորապես նշվեց, որ ընկալումների մակարդակում կարողություններ զարգացնելն, ըստ էության, ավելի բարդ խնդիր է, քան վիրտուալ և ֆիզիկական կարողությունները, որոնց համար ուղղակի պահանջվում են տեխնիկական գիտելիքներ և սարքավորումներ: Ինչպես և վերը հիշատակված Չեխիայի դեպքում, խնդիրը կիբերանվտանգության և դրա կարևորության մասին տեղեկացվածության պակասն է:

Սլովակիա

Սլովակիայի Հանրապետության անվտանգության ռազմավարությունն ընդունվել է 2021 թ.: Այն ևս դիտարկում է կիբերտիրույթը որպես առանձին ոլորտ, որում սակայն հատկապես դժվար է պարզել հարձակվողների ինքնությունը՝ հարձակման մեթոդների և գործիքների կատարելագործման պատճառով:[16] Ռազմավարությամբ առաջնային դեր է վերապահվում համագործակցությանը՝ նաև միջազգային, այդ թվում գործընկեր պետությունների հետ երկկողմանի համագործակցությունը, ինչպես նաև դաշնակիցներից ստացված, վտանգ չներկայացնող տեխնոլոգիաների օգտագործմանը:[17]

Ծրագրի շրջանակում 2022 թ. նոյեմբերի 22-ին տեսակապի միջոցով կազմակերպվել էր քննարկում Սլովակիայի Կիբերանվտանգության ազգային կենտրոնի տնօրեն Ռաստիսլավ Յանոտայի հետ՝ «Կիբերանվտանգությունը Սլովակիայում. օրենսդրական և գործնական խնդիրներ» թեմայով, մասնավորապես ուշադրություն դարձնելով օրենսդրական և գործնական որոշ խնդիրների, այդ թվում՝ կիբերանվտանգության ոլորտում տարբեր գործառույթներ իրականացնող պետական կառույցների միջև իրավասությունների բաժանմանը:[18] Ռ. Յանոտան նաև առաջարկեց, որ կիբերանվտանգության ոլորտի համար պատասխանատու հայ պաշտոնյաների համար կազմակերպվի այց Սլովակիա՝ Սլովակիայի միջազգային զարգացման գործակալության (SlovakAid) կողմից առաջարկվող փորձի փոխանակման շրջանակում: Այս հնարավորությունը լրացուցիչ քննարկվեց նաև 2023 թ. փետրվարին հեղինակի Սլովակիա կատարած գործնական այցի ընթացքում:[19] Հայաստանում լրացուցիչ քննարկումներից հետո

[15] Ibid., p. 21.
[16] Security Strategy of the Slovak Republic, p. 12, https://www.mzv.sk/documents/30297/4638226/security-strategy-of-the-slovak-republic.pdf.
[17] Ibid., p. 18.
[18] Rastislav Janota, 'Cybersecurity governance in Slovakia with focus on legislation and practical questions', online presentation, 22 November 2022, https://centreforpolicystudies.org/gallery/SK_cybersecurity_environment.pdf.
[19] Այցը տեղի էր ունեցել Եվրոպական Միության ֆինանսական օժանդակությամբ՝ Սևծովյան տարածաշրջանի քաղաքացիական հասարակության ներկայացուցիչ փորձագետների շարժունակության հիմնադրամի շրջանակում: Հիմնադրամը տնօրինում է Ռումինիայի հասարակական կազմակերպությունների հանուն զարգացման ֆեդերացիան՝ որպես Սևծովյան տարածաշրջանի հասարակական կազմակերպությունների ֆորումի գլխավոր կոորդինատոր՝ ԵՄ-ի

Սլովակիայի միջազգային զարգացման գործակալությանը կարող է ներկայացվել համապատասխան ծրագրի նախագիծ:

Հակիրճ եզրակացություն

Մարդկային գործոնի՝ մասնավորապես տեղեկացվածության պակասի և անփութության հնարավոր վնասները հաշվի առնելիս, կարելի է նաև նշել. «Արդյունավետ տեղեկատվական անվտանգությունը միավորում է տեղեկատվությունը, ցանցերը և համակարգերը պաշտպանելուն նպատակաուղղված միջոցների մի քանի շերտ: Դրանցից մեկի անարդյունավետությունը հանգեցնում է նաև մյուսների անարդյունավետությանը: Կիբերանվտանգության տեսանկյունից երբեմն դիտարկվում են միայն տեխնիկական միջոցները՝ այդ թվում ծրագրային ապահովման լրացումները, ներխուժման հայտնաբերման համակարգերը, հակավիրուսային ծրագրերը և գաղտնագրումը: Սակայն հաջողված կիբերհարձակումներն առավել հաճախ ոչ թե տեխնիկական բնույթ ունեն, այլ անհատական մակարդակում են: Կիբերանվտանգության առումով առավելագույն խոցելիությունը մարդկային գործոնի հետևանք է»:[20] Իսկ, օրինակ, IBM ընկերության «Cyber Security Intelligence»-ի 2014 թ. գնահատմամբ կիբերանվտանգության հետ կապված պատահարների 95% դեպքերում առկա էին որոշակի մարդկանց կողմից կատարված սխալներ»:[21]

Բացի այդ, պետք է նաև հաշվի առնել, որ ոչ ժողովրդավարական պետությունները և մրցակցային ավտորիտար պետությունները օգտագործում են կիբերանվտանգության խնդիրը, և մասնավորապես «առցանց ինքնիխանությունը», որպես պատրվակ՝ իրենց քաղաքացիներին ճնշելու համար՝ նրանց արտաքին ազդեցությունից և սպառնալիքներից իրապես պաշտպանելու փոխարեն: Դա բնակչությանը վերահսկելու հարմար գործիք է՝ լինի դա «սոցիալական ռեյտինգի» համակարգի թե հոգեբանական մշակման լայնածավալ գործողությունների միջոցով: Այսպիսով, ժողովրդավարական պետությունների համար առկա է կրկնակի մարտահրավեր. նրանք պետք է ապահովեն իրենց կիբերտիրույթների պաշտպանությունը՝ միևնույն ժամանակ երաշխավորելով, որ չեն չարաշահի տեխնիկական միջոցները: Քաղաքացիներին պետք է երաշխավորվի, որ պաշտպանական միջոցները չեն օգտագործվի համատարած հետախուզության նպատակով: Այսպես՝ «Եվրոպացիների՝ մասնավորապես Արևելյան և Կենտրոնական Եվրոպայի բնակիչների 20-րդ դարում ունեցած ամբողջատիրության փորձը հուշում է, որ անհատների իրավունքները պետք է երաշխավորվեն կիբերանվտանգության թե՛ ներպետական, թե՛ միջազգային համակարգերում՝ դրանց կարողությունների աճին զուգահեռ: Ժամանակը չափազանց թանկ է, քանի որ հենց այդ գործընթացներն իրարից առանձնանան և երաշխիքները մղվեն հետին պլան, համակարգը չարաշահելու գայթակղությունը

ֆինանսավորմամբ 2022 թ. հունվարից մինչև 2023 թ. փետրվար իրականացվող «Քաղաքացիական հասարակության հնարավորությունների ընդլայնում՝ հանուն սևծովյան տարածաշրջանում համագործակցության» նախագծի շրջանակում:

[20] Elisa Norvanto, 'The human layer of cybersecurity – the art of social engineering' (quoted from Ugo Emekauwa, 'The human layer of information security defense', 2007), in: *Handbook on Cybersecurity: The common security and defence policy of the European Union*, Vol. V, 2nd edition, 2018, p. 192.

[21] Norvanto, op. cit. (quoted from Fran Howarth, 'The role of human error in successful security attacks', SecurityIntelligence.com, 2014).

կավելանա ցանկացած պետության, քաղաքական գործչի կամ կուսակցության համար»:[22]

Սրա առնչությամբ կարելի է վերհիշել մի դեպք, երբ լրատվական հետաքննությունը նպաստեց Հայաստանում համատարած հետախուզության համակարգի ներդրման փորձի կասեցմանը: 2019-ին «Eurasianet» պարբերականի հրապարակման մեջ բացահայտվել էր, որ դեռևս 2011 թ. «Երևան քաղաքի կառավարման տեխնոլոգիաների կենտրոնին» հանձնարարվել էր ոստիկանության և Ազգային անվտանգության ծառայության հետ համատեղ մշակել «Անվտանգ քաղաք» հայեցակարգը, որի շրջանակում կարող էր ներդրվել նաև արհեստական բանականության միջոցով մարդկանց դեմքերի տարբերակման համակարգ: 2017 թ. սկսվել էին բանակցությունները չինական «Huawei» ընկերության հետ, որոնք հրապարակման պահին դեռևս շարունակվում էին: Հրապարակումից որոշ ժամանակ անց Երևանի քաղաքապետարանից հայտնեցին, որ բանակցությունները դադարեցվել են: Սրան ժամանակին անդրադարձել էր նաև «Ֆրիդոմ Հաուզ» կազմակերպությունը՝ «Freedom on the Net 2020» զեկույցում:[23] Այսպիսով, հարկ է կրկին շեշտել, որ հանրային քննարկումները և որոշումների կայացման թափանցիկությունը ժողովրդավարության կարևորագույն տարրեր են, քանի որ ժողովրդավարությունը չի սահմանափակվում պարբերաբար անցկացվող ընտրություններով:

Հաշվի առնելով կիբերանվտանգությանն առնչվող խնդիրների բարդությունն ու փոխկապակցվածությունը, անհրաժեշտ է կազմակերպել պետական և մասնավոր հատվածների, կրթական և գիտական հաստատությունների միջև՝ ներառելով նաև անհատ օգտատերերին: Սա նախ և առաջ պետք է կատարվի ներպետական մակարդակով՝ միաժամանակ նաև ուսումնասիրելով միջազգային համագործակցության հնարավորությունները:

Սլովակիայի հետ համագործակցության վերը նշված գործնական հնարավորությունից բացի, առկա են թե՛ Վիշեգրադյան քառյակի այլ երկրների հետ երկկողմանի, թե՛ այդ ձևաչափով բազմակողմանի համագործակցության զարգացման հնարավորություններ՝ պետական կառույցների փորձագետների վերապատրաստման և այլ ոլորտներում. սրա վերաբերյալ կարող են կազմակերպվել լրացուցիչ խորհրդակցություններ՝ գործնական իրականացման նպատակով:

Կարճաժամկետ առումով նպատակահարմար է նաև ներդնել Չեխիայի ազգային անվտանգության աուդիտում նշված որոշ միջոցներ՝ պետական կառավարման բոլոր մակարդակներում աշխատակիցների ուսուցումը կիբերանվտանգության և «թվային հիգիենայի» վերաբերյալ, ինչպես նաև տեղեկատվական տեխնոլոգիաների և կիբերանվտագության փորձագետների համար կենտրոնացված ուսումնական հաստատության ստեղծումը:

[22] Feledy, op. cit.
[23] Արմեն Գրիգորյան, «Մասնակցային ժողովրդավարության դիմակայունության ամրապնդումը», էջ 9, 2020 թ., https://transparency.am/hy/publication/301:

Armen Grigoryan

Some characteristics of the Visegrad Four states' cybersecurity policies

The term 'cyber security' is nowadays encompassing virtually all facets of modern technology. We live in a digital era where many critical aspects of our lives depend on the network, computers and other electronic devices, and software. All critical infrastructure such as the banking system, healthcare, electricity supply, air traffic, and so forth, governmental agencies, manufacturing industries use devices connected to the Internet as a core part of their operations. In personal life, we have also become dependent on devices always connected to the Internet, as we use social media, navigation apps, game apps, online shopping and numerous other services.

Technology is increasingly more complicated – and so are cyber attacks. Both inherent risk and residual risk are increasing, driven by global connectivity and usage of cloud services. Interconnectedness of the systems and their technological complexity may pave the way for new, even more sophisticated security threats and related risks, and emerging technologies such as 5G networks, artificial intelligence, quantum technologies, etc., will further add to the technological complexity. The ownership structure of some of the systems also increases the risk of compromising data security and critical infrastructure.

Information, including, but not limited to, personal data, intellectual property, and financial data, is sensitive for unauthorised access or exposure that could have negative consequences. Access to information can be used by malign actors for financial gain, extortion, political or social motives, or just vandalism, and seriously threatens personal privacy, the economy and national security. Thus, cyber security is important because it protects all categories of data from theft and damage, while using tools and processes designed to protect networks and devices from external threats. It can help to prevent data breaches, identity theft, and other types of cybercrime.

Cyber security can be categorised in several sub-domains:

- Network Security involves the use of hardware and software to secure computer networks from unauthorised access, disruptions and misuse.
- Application Security involves protection of the software and devices. It can be achieved by constantly updating the software to ensure its security. Security also depends on all stages of the software design – writing source code, validation, threat modelling, etc.
- Information or Data Security involves implementation of protected data storage and transfer mechanisms to maintain the data privacy.
- Identity management deals with the procedure for determining the level of access allowed to individuals and other users.
- Operational Security involves processing and making decisions on handling and securing data assets.
- Mobile Security involves securing the organisational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats, such as unauthorised access, device loss or theft, malware, etc.
- Cloud Security involves protection of the information stored in the digital environment or cloud services.

- Disaster Recovery and Business Continuity Planning deals with the processes, monitoring, alerts, and plans for responding to malicious activities which may cause the loss of operations or data.[1]

User education is also crucial in cyber security. By raising awareness of potential cyber threats, improving the overall security posture, and complying with regulatory requirements, individuals and organisations can reduce the likelihood of becoming victims of cybercrime.

Armenia's National Security Strategy adopted in 2020 contains a one-page section titled 'Ensuring open and safe information and cyber domains'. It views cyber attacks by foreign states, international terrorist organisations, criminal groups and individuals as threats for information security, and also states that 'information wars, including propaganda, manipulations, fake news, and other disinformation tools are becoming more prevalent, and often target democratic values. In this context, we will work to raise public awareness and media literacy to strengthen the capacity of society and the state to counter such information wars'. Furthermore, the strategy also admits: 'A major challenge is the imperfection of a comprehensive state policy regulating the information and cybersecurity sector, the absence of legislation to ensure the protection of critical information infrastructure, the insufficient level of institutional capacity of computer emergency response teams, and the absence of a national cybersecurity center', and pledges to develop national information and cyber capabilities, including a national cyber security centre and computer emergency response teams.[2]

The formulation of the strategy is advanced compared to the previous version of the National Security Strategy adopted in 2007. However, in practical terms rather modest progress has been achieved. There is still a lack of a comprehensible strategy regarding digital and information security, and that can be observed during crises such as hacker attacks.

At the same time, governmental agencies in charge for cybersecurity policy are open for cooperation with potential partners. The ministry of high-tech industry, besides eagerness to explore the possibilities of cooperation with foreign partners in order to improve the legislation and policy implementation, has also been supporting user education. A recent example is the partnership with the Union of Employers of Information and Communication Technologies for organising an intensive training course, with 30-80% of the participation costs subsidised by the government.[3]

This paper summarises some of the findings of the project implemented by the Centre for Policy Studies with support of the International Visegrad Fund and Ministry of Foreign Affairs of the Republic of Korea. The paper particularly focuses on parts of presentations of the project experts, and additional information that could help to identify the possibilities for improvements in Armenia's cyber security policy and its implementation.

---

[1] 'What is Cyber Security?' https://www.javatpoint.com/what-is-cyber-security.
[2] National Security Strategy of the Republic of Armenia, pp. 29–30, https://www.mfa.am/filemanager/security%20and%20defense/Armenia%202020%20National%20Security%20Strategy.pdf.
[3] https://edu.hti.am/trainings/cybersecurity.

National security strategies and policies in a comparative perspective

Visegrad Four states' national security strategies and policies deriving from them have a lot of similarities. That is unavoidable, given that all four of those countries and NATO and EU members, and harmonisation of most of the policy aspects is a part of their obligations towards NATO, the EU and allied states.

In 2018 European Parliament, the Council and the European Commission reached a political agreement on the Cybersecurity Act, which reinforces the mandate of the EU Agency for Cybersecurity so as to better support Member States with tackling cybersecurity threats and attacks, and also establishes an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices. Yet, regarding the latter, it has been noted: 'As long as foreign-produced software and hardware are present at all levels of life of EU citizens, security can only remain a distant dream'.[4]

Advanced possibilities available to NATO and EU members notwithstanding, Visegrad Four states face challenges similar to those faced by Armenia – hence, some considerable similarities in formulation and, at least theoretically, in some of the approaches. At the same time, a number of advanced-level policies and the structure of some governmental bodies deserve closer attention, and can be considered as best practice examples.

Czech Republic

The national Computer Emergency Response Team (CERT) has been operated since 2011 under the name CSIRT.CZ (CSIRT stands for Cyber Security Incident Response Team). Its powers are determined by Act 181/2014 (Cyber Security Act) and a public contract signed with the National Cyber and Information Security Agency (NÚKIB), which is the cyber security administrator and the central administrative body for cyber security, including the protection of classified information in information and communication systems, cryptographic protection, as well as responsible for non-public services in relation to the Galileo satellite system.[5] NÚKIB also regularly publishes cautionary alerts about current threats and recommendations on its website.

The Security Strategy of the Czech Republic, adopted in 2015, stipulates that, besides the commonly recognised threat of cyber attacks directed against the public and private sectors, there are additional risks for the critical infrastructure, and its protection includes monitoring of foreign investment into critical infrastructure sectors and strategic companies in order to avert the threat of misuse of such investment as a

[4] Botond Feledy, 'Cyber security and Sovereignty: Two levels of digital autonomy'. Think Visegrad policy brief, 2018, https://europeum.org/en/articles/detail/2454/cyber-security-and-sovereignty-two-levels-of-digital-autonomy.

[5] National Cyber Security Strategy of the Czech Republic, p. 7, available at https://nukib.cz/en/cyber-security/strategy-action-plan/.

channel that foreign powers might use to promote their interests. That particularly includes the energy sector and the information and communications technology sector.[6]

The National Security Audit released in 2016 applied a comprehensive strategic review process, analysing the fundamental threats to Czech society, and the weaknesses and gaps in national security. The audit reviewed five specific categories of cyber threats that are of significant importance to national security, namely cyber espionage; disruption or lowering of resilience of IT infrastructure; hostile campaigns; disruption or lowering of security of e-government; and cyberterrorism. According to the threat relevance assessments, the Czech Republic faces high risk of cyber espionage in order to gain strategically sensitive or important information and personal, sensitive, or classified data. There is also high risk of disruption or lowering of resilience of IT infrastructure, and some of the specific risks and challenges in this regard are that state and public administration employees are not sufficiently aware of cybersecurity, lacking education and respect to the basics of 'digital hygiene';[7] and some ministries and institutions' poor prioritisation when planning investment in security technologies and other ICTs. The risks of lowering of security of e-government was estimated as medium-level, with poorly set cybersecurity policies and state administration employees' inadequate awareness as specific risks and challenges. Another medium-level risk is represented by cyberterrorism.[8]

Another specifically focused and recently updated document is the National Cyber Security Strategy of the Czech Republic for 2021-2025 – a comprehensive strategic review process which analysed the fundamental threats to the society and exposed the weaknesses and gaps in national security. It particularly mentions that there are problems associated with transformation into an information society, such as insufficient digital hygiene, media literacy, and critical thinking. Therefore, the state must include cyber security at all levels of the education system and across all fields, emphasising security as a priority when using any electronic device.[9] The National Cyber Security Strategy is accompanied by an action plan, which defines tasks related to cyber security, the bodies responsible for implementation, and timeframes.[10]

Researcher from the Prague-based Institute for Politics and Society, Jan Havlíček, who visited Armenia in December 2022 in the framework of the project organised by the Centre for Policy Studies, mentioned in an interview with the *Aravot* daily that the Czech EU presidency (July – December 2022) organised a high-profile conference about cyber security and Europe's digital future, with representatives of the USA and Australia also present. Under the Czech presidency, the member states also agreed on a common position for negotiations with the European Parliament on enhancing cyber security within EU institutions and bodies. In November, the Council, European Parliament, and the Commission signed up to protecting and promoting European values such as democracy, equality, and sustainability in the digital world. Negotiations between the

[6] Security Strategy of the Czech Republic, https://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf, p. 20.
[7] 'Digital hygiene' is defined as a set of principles, procedures, and habits that allows users to securely move around cyberspace', with a proactive approach by users to their digital footprint, security, etc.
[8] National Security Audit, https://www.mvcr.cz/chh/soubor/national-security-audit.aspx, pp. 97–104.
[9] National Cyber Security Strategy of the Czech Republic, p. 18, available at https://nukib.cz/en/cyber-security/strategy-action-plan/.
[10] Action Plan for the National Cyber Security Strategy of the Czech Republic, available at https://nukib.cz/en/cyber-security/strategy-action-plan/.

Czech Presidency and the European Parliament on product safety were also concluded.[11] The latter is directly related to the abovementioned dilemma posed by foreign-produced software and hardware.

It may additionally be noted that the Czech Republic also prepared the Package on Resilience for the Eastern Partnership, mentioning the need of cooperation for addressing hybrid threats, including cyber attacks. This was particularly mentioned by Jan Plešinger, then the Deputy Head of Mission of the Czech Embassy in Armenia, in an opening address during the 'Czech perspective on the Eastern Partnership' webinar organised on 13 July 2020 as a part of the previous CPS project supported by the International Visegrad Fund.[12]

Hungary

Hungary's cyber security policies were not specifically studied during this project: expert discussions with Hungarian experts focused on several other issues. However, it may be noted that Hungary's National Security Strategy adopted in 2020 regards cyberspace as a separate operational domain alongside land, sea, air and outer space, and considers an extension of future conflicts to cyberspace highly probable. Since cyber capabilities can endanger physical security or cause major material damage, the strategy reserves the right to respond to such attacks in the physical domain, also considering that given the difficulty of attribution and the identification of perpetrators, responses would require particularly careful assessment.[13] This implies that under certain circumstances Article 5 of the NATO Charter, stipulating collective defence, can also be invoked in case of cyber attacks.

The strategy also gives vital importance to strengthening of national cyber defence capabilities based on domestic research and development. Considering that several Hungarian universities have achieved an advanced level of research in applied mathematics and other relevant subjects, it may be particularly recommended to explore possibilities for developing academic cooperation. This opportunity may be a part of the consultations following the agreement to restore the diplomatic relations between Armenia and Hungary.

Poland

The National Security Strategy of the Republic of Poland adopted in 2020 envisages an increase of resilience to cyber threats and of information protection in the public, military and private sectors, particularly, by means of developing national capabilities in

[11] Emma Gabrielyan, 'Hybrid Threats in the Centre of Attention'. *Aravot*, 20 December 2022, https://www.aravot-en.am/2022/12/20/316373/.
[12] 'The Czech Republic will continue supporting Armenia within the Eastern Partnership'. 1in.am, 14 July 2020, https://www.1in.am/2787790.html.
[13] Hungary's National Security Strategy. A Secure Hungary in a Volatile World. https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html#:~:text=83)%20Hungary%20regards%20its%20primary,human%20rights%20and%20fundamental%20freedoms.

the area of testing, research, assessment and certification of cyber security solutions and services. Among the measures towards that goal there is 'development of domestic solutions in the area of cyber security and by conducting state-funded research and development work in the domain of modern technologies, among others, machine learning, the Internet of Things, fixed-line and mobile broadband networks (5G and subsequent generations), including cooperation with universities, scientific institutions and enterprises from both public and private sectors'.[14] The strategy also suggests that in order to ensure secure functioning of the state and its citizens in the information space, there is a need to build capabilities for protection of the information space by merging several layers: virtual (the layer of systems, software and applications), physical (infrastructure and equipment), and cognitive.[15]

It may be noted that, as suggested during a public discussion on Poland's security policy with Wojciech Przybylski, chairman of the Res Publica Foundation and editor-in-chief of Visegrad Insight, during his visit to Yerevan organised within the framework of this project in January 2023, capability building at the cognitive layer can be more difficult than at the layers which primarily require technical knowledge and equipment. The problematic issue, like in the Czech case mentioned above, is the lack of awareness about cybersecurity and its importance.

Slovakia

The Security Strategy of the Slovak Republic was adopted in 2021. It also views the cyberspace as a special operational domain, while, due to the growing sophistication of attacks, it is difficult to reliably attribute the attackers' identity.[16] The strategy prioritises cooperation, including the international level, particularly in the form of bilateral cooperation with partner countries, and the use of technologies coming from partners and allies, which do not pose a security threat.[17]

Within the framework of this project, an online presentation by the director of the National Cyber Security Centre of the National Security Authority of the Slovak Republic, Col. Rastislav Janota, took place on 22 November 2022. The presentation covered cybersecurity governance in Slovakia, with a focus on legislation and practical questions, including the division of responsibilities between governmental bodies dealing with different aspects of cybersecurity.[18] Notably, Col. Janota also suggested that Armenian policymakers responsible for cybersecurity might benefit from the possibility of study visit to Slovakia administered by the Slovak Agency for International Development Cooperation - SlovakAid within the Sharing Slovak Experience programme. This opportunity was discussed in more detail during the author's study visit to Slovakia in

[14] National Security Strategy of the Republic of Poland, p. 20, https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf.
[15] Ibid., p. 21.
[16] Security Strategy of the Slovak Republic, p. 12, https://www.mzv.sk/documents/30297/4638226/security-strategy-of-the-slovak-republic.pdf.
[17] Ibid., p. 18.
[18] Rastislav Janota, 'Cybersecurity governance in Slovakia with focus on legislation and practical questions', online presentation, 22 November 2022, https://centreforpolicystudies.org/gallery/SK_cybersecurity_environment.pdf.

February 2023.[19] After additional discussions with Armenian officials, a project may be submitted to SlovakAid.

Brief conclusion

Regarding the human factor, it has also been noted: 'Effective information security comprises multiple layers of defence which work together to protect information, access to networks and information systems. The premise is that if one layer fails, other layers will fail too. Technical layers such as firewalls, software patches, intrusion detection systems, anti-virus programmes, and encryption are often the only areas that are considered in cyber security. However, effective penetration attacks are often social rather than technical and they account for the majority of cyber attacks. Indeed, the most significant vulnerability in information security relates to human error'.[20] Also, the IBM's Cyber Security Intelligence index estimated in 2014 that 95% of all information security incidents involves human error.[21]

At the same time, it should be remembered that for non-democratic states and competitive autocracies cyber security and, particularly, 'internet sovereignty' is also a pretext to suppress their own population rather than just to defend them from outside influence and threats. It is an easy way for population control, for example, in the form of a social rating system, and for massive psychological operations. Thus, there is a double challenge for democratic states: they need to defend their own citizens in the cyber space and, at the same time, to guarantee that they will not abuse the technical power which is otherwise necessary for their security. Citizens must get all the guarantees that the tools installed for their protection are not transforming into a surveillance society: 'The European – and especially East- and Central European – experience of totalitarianism in the 20th century is a memento that guarantees at individual level must be included in the intra- and international system of cyber security parallel to the development of offensive capabilities. Time is crucial as once these processes get separated and guarantees would lag behind, the temptation would increase for any country, politician or party to abuse the system'.[22]

In this regard, it may be useful to mention a case when media exposure helped to prevent introduction of a mass surveillance technology in Armenia. In 2019, a Eurasianet report revealed that back in 2011 the Yerevan Centre for Management Technologies had been given the task to cooperate with the police and the National Security Service in order to develop a 'Smart City' policy, which would particularly entail deployment of a CCTV network with artificial intelligence-driven facial recognition software. Negotiations with Huawei had been going on since 2017. After the publication,

---

[19] This action was financially supported by the European Union within the framework of the Mobility Fund for CSO Experts within the Black Sea Region, implemented by FOND - the Romanian NGDO Platform as main coordinator of the Black Sea NGO Forum, in the context of the EU-funded project 'Building CSO Capacity for Regional Cooperation within the Black Sea Region' (January 2022 – February 2023).

[20] Elisa Norvanto, 'The human layer of cybersecurity – the art of social engineering' (quoted from Ugo Emekauwa, 'The human layer of information security defense', 2007), in: *Handbook on Cybersecurity: The common security and defence policy of the European Union*, Vol. V, 2nd edition, 2018, p. 192.

[21] Norvanto, op. cit. (quoted from Fran Howarth, 'The role of human error in successful security attacks', SecurityIntelligence.com, 2014).

[22] Feledy, op. cit.

the negotiations were suspended. The issue was also mentioned by Freedom House in the Freedom on the Net 2020 report.[23] So, it can be stated that public discussion and transparent decision making remain vital components of democracy, which cannot be sustained just by means of regular elections.

In view of the complex nature of cyber defence tasks, partnerships must be developed among public and private sector actors, educational and scientific institutions and individual users. This should be done first and foremost on a national level, but the potential of international cooperation should also be identified and explored.

Along with the aforementioned actual possibility of developing cooperation with Slovakia, there are other possibilities of bilateral and multilateral cooperation with the Visegrad Four. That may potentially include study visits for public servants and other types of cooperation. Possible ways of practical implementation may be additionally discussed.

In the short-term perspective, it would be feasible to start implementing some of the measures proposed in the Czech National Security Audit, such as standardising staff training in the field of cybersecurity and digital hygiene at all levels of state authorities, as well as creating a central training facility for high quality technical training of ICT and cybersecurity experts.

[23] Armen Grigoryan, 'Strengthening the resilience of participatory democracy facing authoritarian tendencies', p. 9, 2020, https://transparency.am/hy/publication/301.