



SAJUNGOS VYRIAUSIASIS
ĮGALIOJINIS UŽSIENIO
REIKALAMS IR
SAUGUMO POLITIKAI

Briuselis, 2018 06 13
JOIN(2018) 16 final

**BENDRAS KOMUNIKATAS EUROPOS PARLAMENTUI, EUROPOS VADOVŲ
TARYBAI IR TARYBAI**

Atsparumo didinimas ir kovos su hibridinėmis grėsmėmis pajėgumų plėtra

1. ĮVADAS

Valstybių ir nevalstybinių subjektų hibridinė veikla toliau kelia labai rimtą grėsmę ES ir jos valstybėms narėms. Padažnėjo pastangų silpninti visuomenės pasitikėjimą valdžios institucijomis ir pakirsti pagrindines visuomenių vertybes siekiant destabilizuoti padėtį šalyse. Norintieji pakenkti ES ir jos valstybėms narėms meta mūsų visuomenėms didelius iššūkius, pavyzdžiui, trikdydami ekonomiką ir viešųjų paslaugų teikimą kibernetiniais išpuoliais, imdamiesi tikslinės dezinformacijos kampanijų ar priešiško karinių veiksmų.

Hibridinės kampanijos yra daugiaplanės, joms naudojamos prievartinės ir ardomosios priemonės, tradiciniai ir netradiciniai metodai ir taktika (diplomatiniai, kariniai, ekonominiai ir technologiniai) siekiant destabilizuoti priešininką. Jos parengtos taip, kad būtų sunkiai aptinkamos ar priskiriamos ir gali būti vykdomos tiek valstybių, tiek nevalstybinių subjektų. Kovo mėn. Solsberyje įvykdytas išpuolis naudojant paralyžiuojamąją nuodingąją medžiagą¹ dar akivaizdžiau parodė, kokios skirtingos hibridinės grėsmės ir kiek daug taktikų gali būti taikoma. Į tai reaguodama Europos Vadovų Taryba² pabrėžė, kad tokiose srityse kaip kibernetinė veikla, strateginė komunikacija ir kontržvalgyba reikia didinti ES ir jos valstybių narių pajėgumą aptikti hibridines grėsmes, užkirsti joms kelią ir į jas reaguoti. Ji taip pat atkreipė ypatingą dėmesį į tai, kad reikia būti atspariems cheminių, biologinių, radiologinių ir su branduoline veikla susijusių grėsmių akivaizdoje.

Nekonvencinių ginklų keliamos galimos grėsmės mastas toks, kad ji priskiriama atskirai kategorijai. Juos ne tik sunku aptikti ir priskirti, bet ir sudėtinga atitaisyti jų žalą. Tarptautinei bendruomenei apskritai kelia susirūpinimą ir cheminės, biologinės, radiologinės ir branduolinės grėsmės, kurios apima ne tik hibridines, bet ir terorizmo grėsmes³. Nerimą ypač kelia kintanti rizika, kad vis daugiau šalių įgis branduolinį ginklą ir kad jis gali patekti į nevalstybinių subjektų rankas.

Už didesnę atsparumą šioms grėsmėms ir pajėgumų stiprinimą pirmiausia atsakingos valstybės narės. Vis dėlto ES institucijos jau ėmėsi tam tikrų veiksmų, kurie padėtų sustiprinti nacionalines pastangas. Pavyzdžiui, glaudžiai bendradarbiauta su kitais tarptautiniais subjektais, visų pirma Šiaurės Atlanto sutarties organizacija (NATO)⁴. Siekiant padėti valstybėms narėms tokiose srityse kaip greitis reagavimas, šis darbas galėtų vykti intensyviau⁵.

Šis bendras komunikatas – tai atsakas į Europos Vadovų Tarybos prašymą šį darbą tęsti. Jis yra dalis platesnio priemonių rinkinio, kurį sudaro naujausia pažangos siekiant saugumo sąjungos ataskaita⁶, kurioje apžvelgiama, kaip įgyvendinamas 2017 m. spalio mėn. patvirtintas pasirengimo cheminėms, biologinėms, radiologinėms ir branduolinėms

¹ Dėl išpuolio Solsberyje 2018 m. kovo 22 d. Europos Vadovų Taryba „pritarė Jungtinės Karalystės vyriausybės vertinimui, jog labai tikėtina, kad Rusijos Federacija yra atsakinga ir kad nėra kito įtikinamo paaiškinimo“.

² 2018 m. kovo mėn. Europos Vadovų Tarybos išvados.

³ Pavyzdžiui, 2016 m. gruodžio 14 d. Jungtinių Tautų Saugumo Tarybos rezoliucija S/RES/2325 (2016).

⁴ Kova su hibridinėmis grėsmėmis iš viena iš septynių bendradarbiavimo su Šiaurės Atlanto sutarties organizacija sričių, nurodytų bendrame pareiškime, kurį 2016 m. liepos mėn. Varšuvoje pasirašė Europos Vadovų Tarybos pirmininkas, Europos Komisijos pirmininkas ir Šiaurės Atlanto sutarties organizacijos generalinis sekretorius.

⁵ 2018 m. birželio mėn. Šarlevua vykusiame G 7 aukščiausiojo lygio susitikime taip pat susitarta kurti G 7 greitojo reagavimo mechanizmą, kuris padėtų šalinti grėsmes demokratinėms valstybėms: <https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats/>

⁶ Penkioliktoji pažangos, padarytos kuriant tikrą veiksmingą saugumo sąjungą, ataskaita, COM(2018) 470.

grėsmėms veiksmų planas⁷, ir nurodomi tolesni veiksmai, taip pat antroji pažangos ataskaita⁸, kaip įgyvendinami dvidešimt du komunikato „Bendra kovos su mišriomis grėsmėmis sistema. Europos Sąjungos atsakas“⁹ veiksmai.

2. ES ATSAKAS

Komisija ir Vyriausiasis įgaliotinis nuosekliai dirbdami siekia stiprinti ES pajėgumus ir veiksmingai padėti valstybėms narėms kovoti su hibridinėmis ir cheminėmis, biologinėmis, radiologinėmis ir su branduolinėmis grėsmėmis. Apčiuopiamų rezultatų jau pasiekta tokiose srityse kaip strateginė komunikacija, informuotumas apie padėtį, parengties gerinimas, atsparumo didinimas ir reagavimo į krizes pajėgumų stiprinimas.

Strateginės komunikacijos Rytų kaimynystės šalyse darbo grupė, įsteigta po 2015 m. kovo mėn. Europos Vadovų Tarybos posėdžio, vadovavo darbams, susijusiems su dezinformacijos, atsirandančios iš užsienio šaltinių, prognozavimu ir atsekimu, ir kovai su ja. Jos ekspertizės ir viešai skelbiami produktai¹⁰ žymiai pagerino suvokimą apie Rusijos dezinformacijos poveikį. Per pastaruosius dvejus metus ji padėjo atskleisti daugiau kaip 4 000 atskirų dezinformacijos atvejų, dauguma jų buvo sąmoningai nukreipti prieš Europą. Strateginės komunikacijos Rytų kaimynystės šalyse darbo grupė taip pat siekė, kad rytinėse kaimyninėse šalyse būtų plačiau ir geriau pateikiama pozityvi informacija. Matant šią sėkmę, sukurtos kitos dvi darbo grupės, skirtos skirtingoms geografinėms zonoms – Vakarų Balkanų darbo grupė ir speciali arabų pasauliui skirta Pietų darbo grupė.

Imtasi svarbių veiksmų siekiant sukurti struktūras, kurių reikia norint geriau suvokti padėtį ir priimti pasvertus sprendimus. 2016 m. Europos išorės veiksmų tarnybos ES žvalgybos ir situacijų centre sukurtas Hibridinių grėsmių analizės ir informavimo centras. Hibridinių grėsmių analizės ir informavimo centras priima ir analizuoja įslaptintą ir atvirai prieinamą su hibridinėmis grėsmėmis susijusią informaciją iš įvairių suinteresuotųjų subjektų. Iki šiol jis parengė daugiau kaip 100 vertinimų ir informacinių pranešimų, kurie, siekiant padėti ES priimti pasvertus sprendimus, buvo persiųsti ES institucijoms ir valstybėms narėms. Hibridinių grėsmių analizės ir informavimo centras glaudžiai bendradarbiauja su Helsinkyje įsikūrusiu Europos kovos su hibridinėmis grėsmėmis centru. Šis 2017 m. balandžio mėn. įsteigtas kompetencijos centras skatina strateginį dialogą ir atlieka hibridinių grėsmių mokslinius tyrimus. Dabar jo narėmis jau yra tapusios 16 šalių¹¹. Centras gauna nuolatinę ES paramą.

Taip pat imtasi svarbių žingsnių gerinant parengtį ir atsparumą, ypač cheminėms, biologinėms, radiologinėms ir su branduoline veikla susijusioms grėsmėms. Per pastaruosius šešis mėnesius atlikti dideli darbai – nustatyta pasirengimo cheminiams, biologiniams, radiologiniams ir su branduoline veikla susijusiems saugumo incidentams spragų. Ypač trūksta aptikimo pajėgumų, kurie padėtų užkirsti kelią cheminiams, biologiniams, radiologiniams ir branduoliniams išpuoliams. Komisijos iniciatyva nacionalinių ekspertų konsorciumas išanalizavo, kokios aptikimo įrangos trūktų susiklosčius skirtingiems cheminių, biologinių, radiologinių ir su branduoline veikla

⁷ COM(2017) 610 *final*.

⁸ Bendra ataskaita dėl bendros kovos su hibridinėmis grėsmėmis sistemos įgyvendinimo 2017 m. liepos mėn. – 2018 m. liepos mėn., JOIN(2018) 14.

⁹ JOIN(2016) 18 *final*.

¹⁰ Žr. www.euvtsdisinfo.eu

¹¹ 14 iš 16 narių yra ES valstybės narės: Čekija, Danija, Estija, Ispanija, Italija, Jungtinė Karalystė, Latvija, Lenkija, Lietuva, Nyderlandai, Prancūzija, Suomija, Švedija, Vokietija. Iniciatyva sukurti centrą atsirado įgyvendinant bendros kovos su hibridinėmis grėsmėmis sistemą. Centrą taip pat aktyviai bendradarbiaudamos remia ES ir Šiaurės Atlanto sutarties organizacija.

susijusių grėsmių scenarijams. Trūkumų analizės ataskaita perduota valstybėms narėms, kad jos galėtų priimti informacija pagrįstus sprendimus dėl aptikimo strategijų ir imtis operatyvinių veiksmų, kad nustatytų trūkumai būtų pašalinti.

Šį darbą papildė pratybos, per kurias tikrinta daroma pažanga. 2017 m. kartu su Šiaurės Atlanto sutarties organizacija vykdytos lygiagrečios ir koordinuotos pratybos (PACE17) sudarė sąlygas visapusiškai išbandyti ES pajėgumą reaguoti į didelio masto hibridinę krizę. Precedentų neturinčio masto pratybose išbandyti ne tik „ES hibridinių grėsmių vadovas“, įvairūs ES reagavimo mechanizmai ir jų pajėgumas veiksmingai sąveikauti tarpusavyje, bet ir patikrinta, kaip ES reagavimo į hibridines grėsmes veiksmai sąveikauja su Šiaurės Atlanto sutarties organizacijos veiksmais. Planuojamos 2018 m. pratybos ir siekiama, kad pratybos vyktų kasmet ir padėtų valstybėms narėms stiprinti turimus reagavimo į hibridines krizes gebėjimus.

Šie konkretūs veiksmai rodo, kad ES sukurti politikos modeliai duoda vaisių: per pastaruosius dvejus metus sukurta keletas modelių, kurie suteikia kryptį ir vientisumą ES pastangoms.

2016 m. balandžio mėn. komunikate „*Bendra kovos su mišriomis grėsmėmis sistema. Europos Sąjungos atsakas*“¹² paraginta laikytis principo – kovoti su **hibridinėmis grėsmėmis** ir stiprinti ES, valstybių narių ir tarptautinių partnerių atsparumą visais valdžios lygmenimis – ir nurodytos 22 veiklos sritys. Dauguma tame komunikate apibrėžtų veiksmų siekiama gerinti informuotumą apie padėtį ir didinti atsparumą užtikrinant geresnius reagavimo pajėgumus: numatyta stiprinti ES žvalgybos analitinius gebėjimus ir ypatingos svarbos infrastruktūros objektų apsaugą, didinti kibernetinį saugumą, kovoti su radikalėjimu ir smurtiniu ekstremizmu ir kt. Komunikate taip pat daug dėmesio skirta su kibernetine veikla susijusioms grėsmėms ir kibernetiniams išpuoliams. Kartu su šiuo bendru komunikatu priimtoje antroje ataskaitoje dėl bendros sistemos parodyta apčiuopiama veiksmų įgyvendinimo pažanga ir patvirtinta, kad kovodama su hibridinėmis grėsmėmis ES deda vis daugiau rimtesnių pastangų¹³.

Siekiant **kibernetinio saugumo** svarbus etapas prasidėjo 2018 m. gegužės 9 d. Tai terminas, iki kurio visos ES valstybės narės turėjo perkelti į nacionalinę teisę pirmąsias ES masto teisiškai privalomas kibernetinio saugumo taisykles – Direktyvą dėl tinklų ir informacinių sistemų saugumo. Tai svarbus platesnės 2017 m. rugsėjo mėn. bendrame komunikate „*Atsparumas, atgrasymas ir gynyba: Europos kibernetinio saugumo didinimas*“¹⁴ išdėstytos strategijos elementas. Direktyvoje numatyta konkrečių didelio masto priemonių, kurios labai padėtų sustiprinti ES kibernetinio saugumo struktūras ir pajėgumus. Daugiausia dėmesio skiriama klausimams, kaip stiprinti ES atsparumą kibernetinių išpuolių atveju, kokias veiksmingas atsakomąsias priemones numatyti baudžiamojoje teisėje ir kaip, bendradarbiaujant tarptautiniu mastu, stiprinti stabilumą pasaulyje. Kartu pateiktas pasiūlymas dėl kibernetinio saugumo akto¹⁵, kuriuo siekiama sustiprinti ES lygmens paramą; papildomai parengta keletas pasiūlymų, kurie turi būti apsvarstyti ir įgyvendinti (žr. toliau).

Dezinformacija kenkia mūsų demokratijai, nes varžo piliečių gebėjimą priimti pagrįstus sprendimus ir dalyvauti demokratiname procese. Piliečiams internete prieinamų žinių kiekis ir įvairovė didžiuliai. Tačiau naujos technologijos gali būti naudojamos siekiant skleisti dezinformaciją precedento neturinčiu mastu ir greičiu, nepaprastai kryptingai sėjant nepasitikėjimą ir įtampą visuomenėje. Komisijos komunikate „*Europos kova su*

¹³ Pirmą įgyvendinimo ataskaita (2017 m. liepos mėn.), JOIN(2017) 30 *final*.

¹⁴ JOIN(2017) 450 *final*.

¹⁵ COM (2017) 477, žr. toliau.

*internetine dezinformacija*¹⁶ yra pateiktas europinis dezinformacijos problemos sprendimo modelis ir įvairūs suinteresuotieji subjektai, ypač interneto platformos ir žiniasklaidos įmonės, paraginti imtis priemonių, siekiant įvairių tikslų: didinti skaidrumą, interneto platformų patikimumą ir atskaitomybę, rinkimų procesų saugumą ir atsparumą; puoselėti švietimą ir ugdyti gebėjimą naudotis žiniasklaidos priemonėmis; remti kokybišką žurnalistiką ir kovoti su dezinformacija vykdant strateginę komunikaciją. Tarp pirmųjų konkrečių veiksmų numatytas kovos su dezinformacija kodeksas, kurį iki vasaros turi parengti įvairių suinteresuotųjų subjektų forumas dezinformacijos klausimais ir faktų tikrintojų tinklas. Pirmas suinteresuotųjų subjektų forumo dezinformacijos klausimais susitikimas įvyko 2018 m. gegužės 29 d. ir jame susitarta dėl veiksmų, kurių reikia norint priimti kodeksą 2018 m. liepos mėn. Komisija iki 2018 m. pabaigos įvertins pažangą, padarytą sprendžiant šią problemą, ir nuspręs, ar šioje srityje reikia imtis papildomų priemonių. Numatyta veikla bus suderinta su Strateginės komunikacijos Rytų kaimynystės šalyse darbo grupės veikla ir ją papildys.

Kalbant apie **chemines, biologines, radiologines ir branduolines grėsmes** 2017 m. spalio mėn. Komisijos *veiksmų plane*¹⁷ pasiūlyti 23 konkretūs veiksmai ir priemonės, kuriais siekiama geriau apsaugoti nuo šių grėsmių piliečius ir infrastruktūros objektus, be kita ko, glaudžiau bendradarbiaujant ES ir jos valstybėms narėms, taip pat su Šiaurės Atlanto sutarties organizacija. Šiame plane, kuris yra viena iš saugumo sąjungos priemonių, skirtų apsaugai nuo terorizmo ir atsparumui jam didinti, laikytasi prevencinio požiūrio, grindžiamo principu, kad cheminių biologinių, radiologinių ir su branduoline veikla susijusių grėsmių tikimybė maža, tačiau išpuolio atveju poveikis didelis ir ilgalaikis. Kita vertus, išpuolis Solsberyje ir didėjantis susirūpinimas dėl teroristų kėslų ir gebėjimo pasinaudoti cheminėmis, biologinėmis, radiologinėmis ir branduolinėmis medžiagomis tiek ES¹⁸, tiek už jos ribų rodo, kad cheminių, biologinių, radiologinių ir branduolinių medžiagų keliama grėsmė yra reali. Todėl juolab reikia skubiai iki galo įgyvendinti veiksmų planą, kuriame laikomasi visas pavojaus rūšis apimančio požiūrio ir daugiausia dėmesio skiriama keturiems tikslams: sumažinti galimybę įsigyti cheminių, biologinių, radiologinių ir branduolinių medžiagų; užtikrinti patikimesnį pasirėngimą cheminio, biologinio, radiologinio ir branduolinio saugumo incidentams ir reagavimą į juos; užmegzti stipresnius vidaus ir išorės ryšius su pagrindiniais regioniniais ir tarptautiniais ES partneriais cheminio, biologinio, radiologinio ir branduolinio saugumo klausimais ir gausinti žinias apie cheminės, biologinės, radiologinės ir branduolinės rizikos pavojus. Išsami informacija apie realią pažangą įgyvendinant veiksmų planą pateikta naujausioje saugumo sąjungos pažangos ataskaitoje, priimtoje kartu su šiuo bendru komunikatu.

Galiausiai, siekiant padidinti kovos su hibridinėmis grėsmėmis pastangų veiksmingumą ir aiškiau parodyti ES valstybių narių ir Šiaurės Atlanto sutarties organizacijos (NATO) sąjungininkų vienybę, bendradarbiavimas kovojant su hibridinėmis grėsmėmis įvardytas kaip viena pagrindinių **ES ir NATO bendradarbiavimo** sričių, kaip nurodyta 2016 m. liepos mėn. *Varšuvos bendroje deklaracijoje*¹⁹. Beveik trečdalis visų dabartinių bendrų pasiūlymų dėl bendradarbiavimo susiję su hibridinėmis grėsmėmis²⁰. Glaudžiau

¹⁶ COM(2018) 236 *final*.

¹⁷ COM(2017) 610 *final*.

¹⁸ Europol, „Terrorism Situation and Trend report“ (TE-SAT) 2017, p. 16, skelbiama: www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. Taip pat žr. Cheminio ginklo uždraudimo organizacijos generalinio direktoriaus pareiškimus: www.globaltimes.cn/content/1044644.shtml.

¹⁹ ES ir NATO bendradarbiavimas šiuo metu vyksta remiantis šia Pirmininko J.-C. Junckerio, Pirmininko D. Tusko ir NATO generalinio sekretoriaus Jenso Stoltenbergo pasirašyta deklaracija.

²⁰ 15283/16 ir 14802/17.

bendradarbiaujant šiame rengiamos aprašytosios pratybos ir įgyvendinamas „ES hibridinių grėsmių vadovas“²¹.

3. AKTYVESNIS REAGAVIMAS Į KINTANČIAS GRĖSMES.

3.1. Informuotumas apie padėtį – gebėjimas aptikti hibridines grėsmes

Norint atremti hibridines grėsmes ir į jas reaguoti reikia turėti pajėgumų anksti aptikti iš vidaus ir išorės vykdomą kenksmingą hibridinę veiklą ir jos šaltinius ir suprasti galimus ryšius tarp dažnai iš pirmo žvilgsnio nesusijusių įvykių. Todėl labai svarbu panaudoti visus turimus duomenų srautus, įskaitant žvalgybą iš viešų šaltinių.

Europos išorės veiksmų tarnyboje įsteigtam Hibridinių grėsmių analizės ir informavimo centrui tenka svarbi vienintelės hibridinių grėsmių analizę atliekančios įstaigos funkcija, tačiau jam reikia būtinų kompetencijų, kad galėtų aprėpti visą hibridinių grėsmių spektrą, įskaitant chemines, biologines, radiologines ir branduolines, ir vykdyti kontržvalgybą. Augant kompetencijai, centras galėtų labiau prisidėti prie ES pastangų reaguoti į būsimas krizes ir parengti daugiau su šiomis konkrečiomis sritimis susijusios išsamios civilinės ir karinės žvalgybos medžiagos. Valstybės narės galėtų tai papildyti savo veiksmais: Hibridinių grėsmių analizės ir informavimo centrui teikti daugiau nacionalinių tarnybų žvalgybinės informacijos ir toliau stiprinti sukurtojo nacionalinių centro kontaktinių punktų tinklo gebėjimus teikti ir apdoroti skubią informaciją. Kitame etape valstybės narės galėtų svarstyti, ar teikti daugiau nacionalinių tarnybų žvalgybinės informacijos ES žvalgybos ir situacijų centrui (INTCEN), kad jis galėtų nuodugniau analizuoti galimas grėsmes.

Tolesni veiksmai

- Vyriausiasis įgaliotinis papildys ES hibridinių grėsmių analizės ir informavimo centrą specializuotais cheminių, biologinių, radiologinių ir branduolinių aspektų kontržvalgybos ir kibernetinės analizės komponentais. Valstybės narės raginamos aktyviau teikti žvalgybos duomenis Hibridinių grėsmių analizės ir informavimo centrui esamų ir naujų hibridinių grėsmių analizės reikmėms.
- Komisija, bendradarbiaudama su Vyriausiuoju įgaliotiniu, baigs darbą, susijusį su pažeidžiamumo rodikliais, kad valstybės narės galėtų geriau įvertinti hibridinių grėsmių potencialą įvairiuose sektoriuose. Šis darbas taip pat padės ES analizuoti hibridinių grėsmių tendencijas.

3.2. Aktyvesni veiksmai reaguojant į chemines, biologines, radiologines ir branduolines grėsmes

2017 m. spalio mėn. Kovos su cheminio, biologinio, radiologinio ir branduolinio saugumo grėsmėmis veiksmų planas suteikia pagrindą veikti siekiant stiprinti parengtį ir atsparumą ir gerinti koordinavimą ES lygmeniu. Plano veiksmai apima įvairias valstybėms narėms naudingas priemones, kurios padėtų telkti praktinę patirtį ir kartu stiprinti gebėjimus, keistis žiniomis bei geriausios praktikos pavyzdžiais ir intensyvuoti operatyvinį bendradarbiavimą. Valstybės narės ir Komisija turi bendradarbiauti, kad veiksmų planą įgyvendintų skubiai ir iki galo. Be to, atsižvelgdama į pažangą, pasiektą analizuojant aptikimo pajėgumų trūkumus ir keičiantis geriausios praktikos pavyzdžiais naujai

²¹ SWD(2016) 227 final.

įsteigtoje Cheminio, biologinio, radiologinio ir branduolinio saugumo patariamojoje grupėje, Sąjunga dabar turėtų imtis tolesnių priemonių dėl augančių ir kintančių grėsmių. Ypač reikia su cheminėmis grėsmėmis susijusių priemonių. Pagal darbo, kuriuo apribota prieiga prie sprogstamųjų medžiagų pirmtakų²², pavyzdį ES turi skubiai imtis operatyvinių priemonių, kad geriau kontroliuotų prieigą prie didelės rizikos cheminių medžiagų ir gerintų pajėgumus kuo anksčiau aptikti tokias medžiagas. Valstybės narės taip pat turėtų apsvarstyti galimybę atlikti tolesnę trūkumų analizę ir ištirti esamą situaciją ES lygmeniu, pavyzdžiui, įvertinti atsparumą cheminėms, biologinėms, radiologinėms ir branduolinėms grėsmėms, turimas deaktyvavimo priemones ir metodus. Norint pasirengti cheminiam, biologiniam, radiologiniam ir su branduoline veikla susijusiam išpuoliui ir pašalinti jo padarinius reikia stiprinti valstybių narių, be kita ko, jų civilinės saugos institucijų, bendradarbiavimą ir koordinavimą. Sąjungos civilinės saugos mechanizmas gali labai palengvinti šį procesą ir taip stiprinti Europos kolektyvinius parengties ir reagavimo pajėgumus.

Svarbią šio darbo dalį sudaro tarptautinis bendradarbiavimas, ir ES gali pasinaudoti ryšiais su cheminės, biologinės, radiologinės ir branduolinės kompetencijos centrais, be kita ko, siekti sinergijos su Šiaurės Atlanto sutarties organizacija ir gaivalinių ir žmogaus sukeltų nelaimių prevencijos, pasirengimo joms ir reagavimo į jas programomis, skirtomis regionams pietinėse ir rytinėse kaimyninėse šalyse²³.

²² Siekdama saugumo sąjungos tikslo nesuteikti erdvės teroristų ir nusikaltėlių veiklai, Komisija ėmėsi ryžtingų veiksmų mažinti galimybes gauti sprogstamųjų medžiagų pirmtakų, kurie gali būti naudojami blogiems tikslams – savadarbiams sprogsmenims gaminti. 2017 m. spalio mėn. Komisija pateikė galiojančiomis taisyklėmis pagrįstą rekomendaciją, kokių priemonių neatidėliotina imtis, siekiant išvengti netinkamo sprogstamųjų medžiagų naudojimo (Rekomendacija C(2017) 6950 *final*). Tuo remdamasi, 2018 m. balandžio mėn. Komisija priėmė pasiūlymą persvarstyti ir sugriežtinti Reglamentą (ES) Nr. 98/2013 dėl prekybos sprogstamųjų medžiagų pirmtakais ir jų naudojimo (COM(2018) 209 *final*).

²³ Rytų ir Pietų kaimynystės šalyse rengiami civilinės saugos mokymai ir pratybos pagal regionines gaivalinių ir žmogaus sukeltų nelaimių prevencijos, pasirengimo joms ir reagavimo į jas programas.

Tolesni veiksmai

- ES turėtų svarstyti priemones, kaip užtikrinti, kad būtų laikomasi kovai su cheminiais ginklais skirtų tarptautinių normų ir standartų, įskaitant galimą specialų su cheminiais ginklais susietų ES sankcijų modelį.
- Toliau įgyvendindama Pasirengimo cheminėms, biologinėms, radiologinėms ir branduolinėms saugumo grėsmėms didinimo veiksmų planą, Komisija bendradarbiaus su valstybėmis narėmis, kad iki 2018 m. pabaigos baigtų šiuos veiksmus:
 - parengtų ypatingą grėsmę keliančių cheminių medžiagų sąrašą, kad būtų galima imtis operatyvinių priemonių siekiant sumažinti galimybę jų gauti;
 - užmegztų dialogą su tiekimo grandinės subjektais privačiajame sektoriuje, kad būtų bendradarbiaujama reaguojant į kintančias su cheminėmis medžiagomis, kurios gali būti naudojamos kaip pirmtakai, susijusias grėsmes;
 - paspartintų grėsmės scenarijų peržiūrą ir dabartinių aptikimo metodų analizę, kad būtų patobulintos cheminių grėsmių aptikimo priemonės ir parengtos veiklos rekomendacijos valstybėms narėms siekiant plėsti jų turimus aptikimo pajėgumus.
- Valstybės narės turėtų sudaryti būtiniausių medicininių reagavimo priemonių atsargų, laboratorijų, gydymo ir kitų pajėgumų inventorių. Komisija bendradarbiaus su valstybėmis narėmis, kad reguliariai fiksuotų, kur visoje ES tų atsargų yra, kad išpuolių atveju būtų galima lengviau jų gauti ir skubiai jomis pasinaudoti.

3.3. Strateginė komunikacija – nuosekli informacijos sklaida

Svarbus su hibridinėmis grėsmėmis susijęs uždavinys – ugdyti sąmoningumą ir šviesti plačiąją visuomenę, kad ji atskirtų informaciją nuo dezinformacijos. Remdamasi Strateginės komunikacijos Rytų kaimynystės šalyse darbo grupės, Hibridinių grėsmių analizės ir informavimo centro ir Europos kovos su hibridinėmis grėsmėmis kompetencijos centro patirtimi, taip pat kitais Komisijos veiksmais²⁴, Komisija ir Vyriausiasis įgaliotinis toliau stiprins ES strateginės komunikacijos gebėjimus ir didins jų profesionalumą, užtikrindami sistemingą sąveiką su esamomis struktūromis ir tarpusavio derėjimą. Ši veikla bus plečiama, kad apimtų kitas ES institucijas ir valstybes nares, be kita ko, pasinaudojant dezinformacijos klausimams skirta saugia internetine platforma, apie kurią buvo paskelbta.

Visose ES institucijose ypač svarbu pagerinti koordinavimą ir bendradarbiavimą strateginės komunikacijos klausimais su valstybėmis narėmis, partnerėmis ir tarptautinėmis organizacijomis. Tam reikia pasirengti ir vykdyti pratybas, kol dar nėra kilusios tikros krizės.

Patirtis rodo, kad rinkimų kampanijos laikotarpiai laikomi itin didelės strateginės svarbos ir jautriais taikiniais: puolimas vyksta pasinaudojant internetine erdve ir joje nepaisant tradicinių (fizinį) apsaugos priemonių ir taisyklių, pavyzdžiui, draudimo vykdyti agitaciją tam tikru laikotarpiu, skaidraus finansavimo taisyklių ir kandidatų lygių galimybių. Pavyzdžiui, vyko išpuoliai prieš rinkimų infrastruktūrą ir kampanijos IT sistemas,

²⁴ Komisijos atstovybės, pavyzdžiui, taip pat aktyviai padeda patikrinti faktus ir išsklaidyti mitus. Kai kurios valstybės narės parengė vietos sąlygoms pritaikytas priemones. Pavyzdžiui, *Les Décodeurs de l'Europe* Prancūzijoje, *Falso Vero UE* Italijoje, viešas mitus apie ES sklaidančių karikatūrų konkursas Austrijoje, panaši karikatūrų serija Rumunijoje ir Atstovybės Jungtinėje Karalystėje projektas „*Euromyths A-Z*“. Rengiama ir daugiau tokių projektų.

trečiosios šalys užsuko politiškai motyvuotas masinės internetinės dezinformacijos kampanijas ir vykdė kibernetines atakas siekdamos diskredituoti demokratinį rinkimą ir sumenkinti jų teisėtumą. Siekiant valstybėse narėse didinti informuotumą apie pasirengimą ir reagavimą į kylančias grėsmes, ES lygmeniu dirbama keliomis kryptimis. Taryboje valstybių narių kibernetinio saugumo institucijos²⁵ paskelbs savanoriškai taikomas gaires ir suformuluos geriausios praktikos pavyzdžius, kaip užtikrinti rinkimų technologijų kibernetinį saugumą per visą rinkimų procesą. Ten bus kalbama apie informacines sistemas ir IRT sprendimus, naudojamus rinkėjams ir kandidatams registruoti, balsams rinkti ir skaičiuoti ir rezultatams perduoti, taip pat tiesiogiai su rinkimų rezultatų teisėtumu susijusias pagalbines sistemas.

Hibridinių išpuolių atveju taip pat reikia užtikrinti greitą, patikimą ir nuoseklų visuomenės informavimą. Bet koks cheminis, biologinis, radiologinis ir branduolinis incidentas ar panašus įvykis sukelia visuomenės nepasitenkinimo bangą, nes piliečiams reikia greitų atsakymų. Ypač svarbu vykdyti strateginę pranešimų sklaidą, be kita ko, informuoti tarptautines organizacijas, kad jos galėtų savo ruožtu pradėti įgyvendinti reagavimo planus.

Tollesni veiksmai

- Europos išorės veiksmų tarnyba ir Komisija imsis bendrų veiksmų atitinkamose savo kompetencijos srityse, kad siekiant kovoti su dezinformacija, skleidžiama iš ES vidaus ir iš už jos ribų, ir atgrasyti užsienio šalių vyriausybės nuo priešiško dezinformacijos skleidimo ir hibridinio kišimosi bendradarbiavimas strateginės komunikacijos klausimais būtų labiau struktūrinis.
- Komisija rudenį organizuos aukšto lygio renginių valstybėms narėms ir atitinkamiems suinteresuotiesiems subjektams. Vienas iš renginių – demokratijai skirtas pagrindinių teisių kolokviumas, kuriuo siekiama skatinti taikyti geriausios praktikos pavyzdžius ir gaires, kaip švelninti per internetą keliamas ir dezinformacijos grėsmes rinkimams ir kaip į jas reaguoti.
- Vyriausiasis įgaliotinis ir Komisija nagrinės būdus, kokiomis priemonėmis ir kokiais ištekliais geriau prisidėti prie trijų strateginės komunikacijos darbo grupių atliekamo darbo siekiant užtikrinti, kad reaguojant į kompleksiškas priešiškas nusiteikusių subjektų vykdomas dezinformavimo kampanijas ES pastangos būtų pakankamo masto.

3.4. Atsparumo ir atgrasomųjų priemonių stiprinimas kibernetinio saugumo srityje

Kibernetinis saugumas yra būtinas tiek mūsų gerovei, tiek saugumui. Mūsų kasdienis gyvenimas ir ekonomika tampa vis labiau priklausomi nuo skaitmeninių technologijų, todėl mums kyla vis daugiau grėsmių.

Veiksmingai užtikrinti kibernetinį saugumą ES šiuo metu trukdo investicijų trūkumas ir nepakankamas koordinavimas. ES dabar siekia šias problemas spręsti ir stiprina pajėgumus: taiko paramos priemones, geriau koordinuoja veiklą ir kuria naujas struktūras,

²⁵ Prižiūrint bendradarbiavimo grupei, įsteigtai pagal Direktyvą dėl tinklų ir informacinių sistemų saugumo.

kurios padėtų tobulinti kibernetinio saugumo technologijas ir jas diegti²⁶. Direktyva dėl tinklų ir informacinių sistemų saugumo²⁷ nustatytas minimalus tinklų ir informacinių sistemų saugumo lygis visoje Sąjungoje. Siekiant padidinti kibernetinį atsparumą, labai svarbu direktyvą iki galo įgyvendinti visose valstybėse narėse. Tai pirmas esminis žingsnis. Bendrajame duomenų apsaugos reglamente nustatytas įpareigojimas pranešti apie asmens duomenų saugumo pažeidimą kompetentingai priežiūros institucijai. Kitos svarbios priemonės – sustiprinta ir modernizuota Europos Sąjungos kibernetinio saugumo agentūra ir vartotojų pasitikėjimą padidinsianti IRT produktų ir paslaugų ES sertifikavimo sistema²⁸. Be to, valstybių narių kompetencijos centrams teikiama parama, kad būtų kuriami ir diegiami kibernetinio saugumo sprendimai ir papildomos ES ir nacionalinio lygmens pastangos stiprinti šios srities pajėgumus. Tuo tikslu bus pasinaudota birželio 6 d. Komisijos pateikta programa „Skaitmeninė Europa“²⁹, kurioje ES investicijoms į kibernetinį saugumą suteikiamas naujas prioritetas.

Be to, Rekomendacijoje dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes³⁰ išdėstyta, kaip turėtų vykti valstybių narių ir įvairių ES subjektų bendradarbiavimas reaguojant į didelio masto tarpvalstybinį kibernetinį išpuolį. Rekomendacijoje pabrėžta, kad siekiant veiksmingo techninio, operatyvinio ir strateginio (politinio) koordinavimo ypač svarbu užtikrinti informuotumą apie padėtį. Pagal Direktyvą dėl tinklų ir informacinių sistemų saugumo įsteigta bendradarbiavimo grupė taip pat stengiasi intensyvuoti susijusių šalių keitimąsi ir dalijimąsi informacija ir rengia bendrą incidentų apibūdinimo taksonomiją. Šis modelis bus patikrintas per būsimas pratybas. Hibridinių grėsmių analizės ir informavimo centras, remdamasis valstybių narių žvalgybos tarnybų informacija, teikia strateginę esamų ir kintančių kibernetinių grėsmių analizę.

Bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistema (Kibernetinio saugumo diplomatijos priemonių rinkinys) iš esmės pagerino operatyvines sąlygas, nes suteikia pagal bendrą užsienio ir saugumo politiką nustatytas priemones (įskaitant ribojamąsias priemones), kuriomis galima sustiprinti ES atkirtį veiklai, kuri kenkia jos politiniams, saugumo ir ekonominiams interesams. Juo daugiau valstybės narės tomis priemonėmis visapusiškai naudosis, tuo efektyvesnis bus jų atgrasomasis poveikis. Balandžio mėn. Užsienio reikalų taryba priėmė išvadas dėl kibernetinės kenkimo veiklos, kuriose griežtai pasmerkė kenkėjišką informacinių ir ryšių technologijų naudojimą, be kita ko, išpuolius *WannaCry* ir *NotPetya*, kurie padarė didelės žalos ir ekonominių nuostolių Europos Sąjungoje ir už jos ribų.

ES ir jos valstybės narės turi padidinti savo pajėgumus nustatyti kibernetinių išpuolių vykdytojus, be kita ko, aktyviau dalydamosi žvalgybos informacija. Vykdytojų nustatymas atgrasytų galimus agresorius ir padidintų tikimybę, kad tie subjektai tinkamai atsakys už savo veiksmus. Didinti atgrasomąjį poveikį yra vienas iš svarbiausių Komisijos strateginio požiūrio į kibernetinio saugumo didinimą tikslų. Neseniai Komisijos pateikti pasiūlymai, kuriais siekiama pagerinti tarpvalstybinį elektroninių įrodymų rinkimą baudžiamojo proceso reikmėms, labai padidintų teisėsaugos institucijų pajėgumą tirti kibernetinius nusikaltimus ir už juos patraukti baudžiamojon atsakomybėn.

²⁶ Vykdamas inovacijų skatinimo Europos regionuose planus, 2017 m. gruodžio mėn. pradėta naujas ES regionus siejantis tarpreregioninis bandomasis projektas, kuriuo siekiama paspartinti darbą kibernetinio saugumo srityje.

²⁷ 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti. COM(2017) 477.

²⁸ Pasiūlymas dėl reglamento dėl Skaitmeninės Europos programos sudarymo 2021–2027 m. laikotarpiui, COM(2018) 434.

³⁰ C(2017) 6100.

Siekiant padidinti kibernetinį atsparumą reikia plataus masto kolektyvinio požiūrio. Todėl reikalingos tvirtesnės ir veiksmingesnės kibernetinį saugumą propaguojančios struktūros, kurios duotų atkirtį kibernetiniams išpuoliams valstybėse narėse, taip pat pačios ES institucijose, agentūrose, delegacijose, misijose ir operacijose: tai, kad nėra visoms Europos institucijoms bendro saugių ryšių tinklo, yra didelis trūkumas. Reikia gerinti ES institucijų ir jų darbuotojų suvokimą apie kibernetinį saugumą – ugdyti saugumui svarbius įgūdžius ir rengti daugiau šios srities mokymų.

Tollesni veiksmai

- Europos Parlamentas ir Taryba turėtų sparčiau dirbti, kad iki metų pabaigos būtų užbaigtos derybos ir susitarta dėl kibernetinio saugumo pasiūlymų, ir greitai susitarti dėl siūlomų teisės aktų dėl elektroninių įrodymų rinkimo.
- Komisija ir Vyriausiasis įgaliotinis glaudžiai bendradarbiaus su valstybėmis narėmis siekdami tobulinti ES masto krizių valdymo ir reagavimo į jas mechanizmų kibernetinius aspektus. Valstybės narės raginamos tęsti savo darbą, susijusį su kibernetinių išpuolių vykdytojų nustatymu ir praktiniu Kibernetinio saugumo diplomatijos priemonių rinkinio naudojimu, kad politinis atsakas į kibernetinius išpuolius būtų griežtesnis.
- Reaguojant į poreikį stiprinti mūsų kibernetinės gynybos pajėgumus, kuriama speciali mokymo ir švietimo platforma, kuri padėtų koordinuoti valstybių narių siūlomas kibernetinės gynybos mokymo galimybes. Reikėtų siekti sinergijos su panašiomis Šiaurės Atlanto sutarties organizacijos pastangomis.

3.5. Didinti atsparumą priešiška žvalgybos veiklai

Kovojant su priešiška žvalgybos veikla visų pirma reikia aktyviau ir veiksmingiau koordinuoti valstybių narių veiksmus, laikantis atitinkamų ES ir nacionalinių taisyklių ir tvarkos. Tačiau taip pat būtina didinti ES institucijų pajėgumus kovoti su augančia konkrečiai prieš institucijas nukreiptos veiklos grėsme ir ugdyti dėmesį saugumui, kartu gerinant mokymą ir rūpinantis fiziniu saugumu. Institucijos taip pat galėtų bendradarbiauti su valstybėmis narėmis, kad būtų sukurta patikimesnė ES akreditavimo sistema. Tokia sistema būtų grindžiama iniciatyviai vykdoma informavimo veikla, kuri padėtų valstybėms narėms ir institucijoms geriau pažinti subjektus, kurie gali būti priešiška nusiteikę, visų pirma tuos, kuriuos jau nustatė valstybės narės.

Koordinuojant valstybių narių veiksmus ir valstybių narių bei kitų svarbių tarptautinių organizacijų, visų pirma Šiaurės Atlanto sutarties organizacijos, veiksmus būtų lengviau pagerinti kontržvalgybą, nukreiptą prieš Europos Sąjungoje vykdomą priešišką veiklą. Viena iš sričių, kurioje prasminga geriau koordinuoti valstybių narių veiklą, yra investicijų tikrinimas remiantis 2017 m. rugsėjo mėn. Komisijos pasiūlytu reglamentu³¹, kuriuo valstybėms narėms leidžiama tikrinti tiesiogines užsienio investicijas saugumo ar viešosios tvarkos sumetimais. Geriau koordinuoti valstybių narių veiklą tiek pat svarbu tikrinant finansinius sandorius, nes priešiškos žvalgybos tarnybos vis dažniau, finansuodamos aktyvias prieš ES nukreiptas priemones, naudoja subtiliomis finansinėmis schemomis.

³¹ Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatoma tiesioginių užsienio investicijų į Europos Sąjungą tikrinimo sistema, COM(2017) 487.

Tolesni veiksmai

- Europos išorės veiksmų tarnyba (EIVT) ir Komisija imsis patobulintų praktinių priemonių, kuriomis siekiama palaikyti ir plėtoti ES gebėjimą bendradarbiauti su valstybėmis narėmis kovoje su priešiška žvalgybos veikla, nukreipta konkrečiai prieš institucijas.
- Sustiprintas Hibridinių grėsmių analizės ir informavimo centras įgis daugiau kontržvalgybos kompetencijos, kad galėtų teikti išsamias analizes ir instrukcijas, kokio pobūdžio priešiška žvalgybos veikla gali būti nukreipta prieš asmenis ir institucijas.
- Europos Parlamentas ir Taryba turėtų sparčiau dirbti, kad iki metų pabaigos būtų užbaigtos derybos dėl investicijų tikrinimo pasiūlymo.

4. IŠVADA

Hibridinės ir cheminės, biologinės, radiologinės ir su branduoline veikla susijusios grėsmės yra viena svarbiausių ES aktualijų. Kovo mėn. Jungtinėje Karalystėje įvykęs incidentas parodė, koks įvairialypis yra hibridinis karas ir kaip ypač reikia būti atspariems cheminių, biologinių, radiologinių ir su branduoline veikla susijusių grėsmių akivaizdoje.

Komisija ir Vyriausiasis įgaliotinis priėmė ir pasiūlė keletą iniciatyvų, kuriomis siekiama reaguoti į hibridinių grėsmių keliamus iššūkius. Komisija taip pat sparčiau įgyvendina 2017 m. veiksmų planą, kad būtų geriau pasirengta rizikai, kuri kyla cheminiam, biologiniam, radiologiniam ir branduoliniam saugumui.

Šiuo bendru komunikatu siekiama informuoti Europos Vadovų Tarybą apie jau vykdomus darbus ir nustatyti sritis, kuriose reikėtų veikti aktyviau siekiant, kad svarus ES įnašas šalinant šias grėsmes taptų dar nuoseklesnis ir didesnis. Valstybės narės, Komisija ir Vyriausiasis įgaliotinis dabar turi skubiai imtis tolesnių veiksmų.