SIGURIA KIBERNETIKE DHE PËRGJIGJET SHUMËAKTORIALE NDAJ KËRCËNIMEVE DHE TERRORIZMIT KIBERNETIK

Përmbledhje praktikash dhe legjislacioni

2024

Instituti për Aktivizëm
dhe Ndryshim Social

Ky studim është produkt i programit "Siguria kibernetike një kërcënim modern për demokracinë", zbatuar nga Instituti për Aktivizëm dhe Ndryshim Social, mbështetur nga Ambasada e Shteteve të Bashkuara të Amerikës, përmes Programit të Granteve të Vogla të Komisionit për Demokraci

Instituti për Aktivizëm dhe Ndryshim Social
Rruga Sulejman Delvina, p2/3, apt.1, Tiranë www.ians-albania.org

Tabela e lëndës

1. Hyrje

Studime dhe analiza e kërcënimeve dhe sulmeve kibernetike tregon se autorë që mund të prodhojnë të tilla ngjarje të rënda me impakt të gjerë publik janë shtete, grupe të krimit të organizuar dhe aktorë të tjerë joshtetërore (terroristët). Përmes Rezolutës nr.2341 (2017), Këshilli i Sigurimit i OKB-së thekson domosdoshmërinë për përgatitje dhe përgjigje ndaj varësisë kibernetike të shoqërive, e cila shfrytëzohet gjerësisht nga grupet terroriste. Këshilli i Sigurimit u bën thirrje shteteve anëtare të investojnë për mbledhjen dhe ruajtjen e provave digjitale ndaj përgjegjësve të sulmeve terroriste dhe mënyrës së përdorur për shfrytëzimin e teknologjisë së komunikimit të informacionit (TIK) nga ana e terroristëve[1]. Këshilli thekson se si mbrojtja e infrastrukturës kritike kundër sulmeve terroriste kërkon përpjekje shumëplanëshe që lidhet me sigurinë mbrojtëse të shteteve, përfshirë këtu dhe sigurinë kibernetike[2]. OKB, nga ana tjetër, ngre alarmin se, "grupet terroriste po fitojnë kapacitete për të nisur sulme terroriste përmes internetit, për dëmtimin e infrastrukturës kritike, sistemeve të kontrollit industrial ose pajisjet IoT (Internet of Things)[3].

> "Grupet terroriste kanë fuqizuar kapacitetin e tyre për sulme terroriste përmes internetit, e për pasojë, dëmet në infrastrukturën kritike, sistemet e kontrollit industrial ose pajisjet dhe Internet of Things (IoT) janë të ndjeshme dhe shpesh të pariparueshme".
>
> *Fleta informuese "Për teknologjitë e informacionit dhe komunikimit", OKB*

Krahas sulmeve kibernetike, një kërcënim faktik përfaqëson edhe terrorizmi kibernetik ose terrorizmi nëpërmjet përdorimit te internetit. Ai paraqitet sporadik për shkak të aftësive teknike specifike për të ndërmarrë një sulm të tillë. Komuniteti ndërkombëtar i njeh dhe u jep përparësi këtyre çështjeve përmes programit global kundër terrorizmit lidhur me sigurinë kibernetike dhe teknologjitë e reja, i cili zbatohet nga Zyra e OKB-së kundër Terrorizmit. Ky program shërben si një instrument për të mbështetur shtetet anëtare në forcimin e kapaciteteve të tyre për të zhvilluar dhe zbatuar një përgjigje efektive ndaj këtij kërcënimi dinamik[4]. Morisë së institucioneve dhe mekanizmave raportues për masat parandaluese i shtohet edhe Zyra e OKB-së për Çështjet e e cila bashkërendon zhvillimet në fushën e informacionit dhe telekomunikacionit, në kontekstin e sigurisë globale Çarmatimit, përmes takimeve në nivel ekspertësh qeveritarë.[5]

---

[1] United Nations Security Council Counter Terrorism Committee Executive Directorate (CTED) (Unknown). 'Information and Communications Technologies Factsheet'. (Accessed online).
[2] United Nations (2017). Security Council Resolution 2341, p. 2. (Accessed online).
[3] United Nations Security Council Counter Terrorism Committee Executive Directorate (CTED) (Unknown). 'Information and Communications Technologies Factsheet'. (Accessed online).
[4] NOCT (Unknown). 'Cybersecurity'. (Accessed online).
5 United Nations (no date). 'Developments in the Field of Information and Telecommunications in the Context of International Security', UN Office of Disarmament Affairs. (Accessed online).

Pavarësisht njohurive dhe informacionit të deritanishëm mbi kërcënimet, rrezikun për sulme apo vetë sulmet kibernetike (terroriste ose jo); masat e ndërmarra nga shtetet (e përmes politikave dhe kuadrit rregullator të caktuar) si dhe nga strukturat e sigurisë kombëtare nuk kanë garantuar në praktikë gatishmërinë e të gjithë aktorëve që preken nga këto kërcënime dhe rreziqe për sulme. Këtu bëhet fjalë për qytetet në funksionimin e të cilave gjenden objekte të infrasktrukturës kritike, shërbime jetike për popullatën si p.sh., shërbimet shëndetësore, ujësjellësat, transporti, bankat apo bizneset lokale[6]. Në këtë raport infrastruktura kritike në komunitet, në qytet apo rajon vlerësohet si pjesë e rëndësishme e funksionimit të komunitetit, qytetit dhe qytetarëve apo rajonit të caktuar; krahas përcaktimit si komponent thelbësor i sigurisë kombëtare. Për këtë arsye, qasja analitike orientohet drejt përgatitjes qytetare dhe institucionale, ndërgjegjësimit dhe diskutimit për përmirësime ligjore në lidhje me rreziqet e mundshme të terrorizmit kibernetik.

Gjithashtu, këtu bëhet fjalë për nevojën për informim dhe ndërgjegjesim të vazhdueshëm qytetar, për rrezikun e mundshëm ndaj sulmeve kibernetike dhe përgatitjen e paneve vendore të përgjigjeve, në reduktimin e impaktit të këtyre sulmeve tek qytetari si përdorues fundor i gjithë të mirave, shërbimeve dhe objekteve që konsiderohen si infrastrukturë kritike. Në këtë mënyrë, ky raport synon të angazhojë autoritetet (qendrore dhe vendore) në përmirësimin e masave parandaluese ndaj një sërë kërcënimesh kibernetike, përmes prezantimit të disa praktikave ndërkombëtare në mënyrën e menaxhimit operacional të sulmeve kibernetike dhe sulmeve kibernetike terroriste; si dhe, për përpjekjet në reduktimin e rreziqeve për sulme të tilla.

Nevoja për të rritur gatishmërinë ndaj sulmeve kibernetike, sidomos ndaj atyre sulmeve me impakt të gjerë në botën reale, është mesazhi kryesor i këtij raporti. Një strategji e qëndrueshme dhe sistematike që synon mbrojtjen dhe garantimin e funksionimit të sistemeve kibernetike dhe që i adresohet qyteteve/bashkive që administrojnë pjesë kryesore të infrasktukturës kritike; si dhe, përfshirja dhe përgatitja qytetare për të rritur gatishmërinë në kundërpërgjigje, është thelbësore

[6] Hill, S., Creese, S. (2021). 'Why Cyber Resilience Must be a Top-Level Leadership Strategy', CAPCO Institute Journal 53: operational resilience (May), p. 82. (Accessed online).

në kushtet aktuale për autoritetet shtetërore. Me rëndësi për këtë gatishmëri duhet të paraqitet, gjithashtu, ekuilibri delikat ndërjet shfrytëzimit të përfitimeve të hapësirës kibernetike dhe teknologjisë vis-a-vis garantimit të sigurisë dhe gatishmërisë në rast sulmesh. Kjo nevojë ndërlidhje së sigurisë kibernetike me sigurinë fizike konsoderohet evolucioni i së ardhmes së përbashkët[7] të njerëzimit.

Fokusi parësor

Hapësira kibernetike dhe gjithnjë e më shumë AI, janë bërë themeli i teknologjive të përditshme. Hapësira kibernetike mund të përkufizohet si një "mjedis kompleks që rezulton nga ndërveprimi i njerëzve, softwerëve dhe shërbimeve në internet me anë të pajisjeve teknologjike dhe rrjeteve të lidhura me të, që nuk ekziston në asnjë formë fizike[8]. Kjo hapësirë fluide, e paprekshme, bëhet gjithnjë e më sfiduese kur përdoruesit, pajisjet, sistemet dhe proceset, gjithnjë e më shumë, lidhen dhe ndërveprojnë me njëri-tjetrin. Ndaj, përdorimi i hapësirës kibernetike, inteligjencës artificiale (AI) dhe teknologjitë e avancuara mund të dëmtojnë shoqëritë nëse përdoren për qëllime keqdashëse nga aktorë armiqësorë. Strategjia e Sekretarit të Përgjithshëm të OKB-së për teknologjitë e reja pranon rreziqet e mëdha që sjellin këto teknologji. Strategjia thekson se "ndërsa hapësira kibernetike ka hyrë pothuaj në çdo aspekt të përditshmërisë, shkalla dhe përhapja e 'pasigurisë kibernetike' njihet gjithashtu si një shqetësim serioz.

Raporti i Komisionit Evropian "The Landscape of Hybrid Threats: A Conceptual Model" eksploron fusha të ndryshme të kërcënimeve hibride, duke përfshirë dhe kërcënimet kibernetike. Në këtë raport theksohet gjithashtu se "çdo gjë me rëndësi në botën reale ndodh njëlloj edhe në hapësirën kibernetike; dhe për pasojë, dimensioni kibernetik luan një rol të jashtëzakonshëm". Raporti është i qartë në deklaratën e tij se "Hapësira kibernetike ofron një mekanizëm të ri shpërndarjeje që mund të rrisë shpejtësinë, përhapjen dhe fuqinë e një sulmi dhe të sigurojë anonimitetin dhe pazbulueshmërinë. Vlera e ulët në përdorim, anonimiteti dhe asimetria në cënueshmëri do të thotë se aktorët më të vegjël kanë më shumë kapacitet për të ushtruar pushtet në hapësirën kibernetike krahasuar me fusha më tradicionale të politikës botërore" [9]
Në një botë ku krimi kibernetik i nivelit të ulët po kthehet në një realitet të ri rrezikshmërie, kushdo që ka akses në sistemet kompjuterike ose pajisjet celulare do të jetë i vetëdijshëm për mashtrimet me anë të "phishing", sulmet me "malware" (në veçanti të tipit "ransomware") që bombardojnë përdoruesit çdo ditë. Kjo pikëpamje, që mbështetet gjerësisht nga Interpol[10], thekson mënyrën sesi krimi kibernetik përparon me një ritëm shumë të shpejtë, me rrjete komplekse kriminale, që veprojnë në mbarë botën dhe që koordinojnë sulme komplekse që mund të ekzekutohen në pak minuta[11]
Siç paralajmëron Shërbimi Kombëtar i Sigurisë në Mbretërinë e Bashkuar, këto kërcënime më pak të dukshme kanë potencialin të na prekin të gjithëve, duke përfshirë shërbimet publike – madje duke sjellë

[7] Barnard, P. (2020). 'Martyn's Law in a Security Convergent World', IFSEC Global. (Accessed online).
[8] ISO (2012). 'ISO/IEC 27032:2012: Information Technology – Security Techniques – Guidelines for Cybersecurity'. (Accessed online).
[9] Giannopoulos, G., Smith, H., Theocharidou, M. (2020). 'The Landscape of Hybrid Threats: A conceptual model', European Commission, Ispra, p. 28 (Accessed online).
[10] ISO (2012). 'ISO/IEC 27032:2012: Information Technology – Security Techniques – Guidelines for Cybersecurity'. (Accessed online).
[11] Interpol (no date). 'Cybercrime'. (Accessed online).

impakt të drejtpërdrejtë në jetën dhe dinjitetin njerëzor[12].
Krahas këtij indikatori specifik, shtetet midis tyre apo në përballjen e tyre me grupet kriminale jo-shtetërore dhe individët, mund të zhvillojnë qasje destabilizuese për shkak të qëndrimeve akuzuese në përcaktimin e përgjegjësisë për sulmet kibernetike.[13]
Sulmet kibernetike mund të përdoren si taktikë nga çdo aktor armiqësor. Edhe pse shtetet njihen për nivele më të larta të aftësive sulmuese kibernetike, mendohet se aktorët joshtetërorë kryejnë shumicën e sulmeve kibernetike, qoftë për veten e tyre apo për një shtet që nuk dëshiron të zbulojë sponsorizimin e sulmit. [14]
Përmes rasteve studimore ndërkombëtare, të identifikuara për kontektin e këtij raporti, synohet shpjegimi i mënyrave jokonvencionale të sulmeve kibernetike, të cilat po shndërrohen në instrumente të një lufte hibride ndërmjet paqes dhe konfliktit; dhe, po përdoren njëlloj si nga aktorë shtetërorë ashtu dhe nga aktorë jo-shtetërorë apo individë.

Financimi i sulmeve terroriste përmes internetit, sillet në këtë raport, si një kërcënim ndaj hapësirës kibernetike dhe nevojë për rregullim ligjor specifik në Shqipërinë.

[12] McCallum, K. (2021). 'Director General Annual Threat Update', UK Security Service MI5. (Accessed online).
[13] United Nations (2018). UN Secretary General's Strategy on New Technologies, pp. 8-9. (Accessed online).
[14] Kreps, S. (2021). 'Democratizing Harm: Artificial Intelligence in the Hands of Nonstate Actors', Brookings Institute, p. 8.

1.1. Terminologjia dhe interpretimi

Në kontekstin e këtij raporti, terminologjia e përshtatur në paketën ligjore mbi sigurinë kibernetike dhe strukturat e mekanizmat rregullues do të pranohet dhe citohet sikundër përcaktohet në këtë paketë ligjore. Në vijim, ky raport ofron një përpjekje për interpretimin dhe përkufizimin e termave specifikë që ende debatohen në diskursin ndërkombëtar mbi rreziqet dhe sulmet kibernetike dhe sulmet kibernetike terroriste.

Kërcënimi kibernetik mund të kuptohet si <u>një rrethanë ose ngjarje me potencial për të ndikuar negativisht në veprimtarinë operative të institucioneve, asetet ose individët nëpërmjet aksesit të paautorizuar në sisteme për shkatërrimin, zbulimin dhe modifikimin e informacionit dhe/ ose mohimin e shërbimit publik</u>[15].
Në këtë drejtim, kërcënimi për sulme kibernetike terroriste ndaj infrastrukturës kritike merr rëndësi specifike[16].

Rrezik i sigurisë kibernetike, një ngjarje e identifikueshme me efekt të mundshëm negativ për sigurinë e rrjeteve e të sistemeve të informacionit.

Sulm kibernetik mund të kuptohet si "përdorim i hapësirës kibernetike me qëllim të ndërprerjes, çaktivizimit, shkatërrimit ose kontrollit me qëllim dëmtues dhe kriminal të një mjedisi/ infrastrukture kompjuterike; ose shkatërrim i integritetit të të dhënave ose vjedhja e informacionit të kontrolluar"[17]. Sulmi kibernetik mund të kuptohet, gjithashtu, si një ngjarje ose situatë që shkakton dështim të sistemeve elektronike të TIK-ut, që kërcënon për dëm serioze për mirëqenien e njerëzve, mjedisin, ofrimin efektiv të shërbimeve kritike publike ose sigurinë kombëtare[18].

Ndaj, në kontekstin e këtij raporti, një sulm kibernetik i referohet në mënyrë specifike atyre veprimeve të qëllimshme, të paligjshme dhe domethënëse që depërtojnë, shfrytëzojnë dhe/ose ndikojnë ose cënojnë infrastrukturën kritike, shërbimet thelbësore dhe funksionimin efektiv të qyteteve, me implikime tek qytetari si përdorues fundor i strukturave dhe shërbimeve (pavarësisht autorit të sulmit).

Termi **"terrorizëm kibernetik"** u krijua në fund të viteve 1980 që kombinon sëbashku terrorizmin dhe hapësirën kibernetike[19]. Në kontekstin e sulmeve të Qendrës Botërore të Tregtisë në 1993, bombardimeve në Oklahoma në 1997 dhe bombardimeve të ambasadave të SHBA në Kenia dhe Tanzani në 1998, hapësira kibernetike u pa si një vektor potencial për të cënuar shoqëritë e lidhura përmes internetit. Në këtë sfond, referenca e parë për këtë çështje vjen përmes një dokumenti politik "*Terrori kibernetik: Perspektivat dhe Implikimet*" (1999) [20], i cili është studimi i parë gjithëpërfshirës që trajtoi

[15] Computer Security Resource Centre Glossary (no date). 'Cyber threat'. (Accessed online).
[16] United Nations (2017). Security Council Resolution 2341. (Accessed online).
[17] Computer Security Resource Centre (no date). 'Cyber Attack' definition, National Institute of Standards and Technology.
[18] Lobel-Weiss, N., Gould, T. (2019). London Cyber Incident Response Framework, London Resilience, p. 5.
[19] Emery, N.E. (2005). 'The Myth of Cyberterrorism', Journal of Information Warfare, 4(1), pp. 80-89
[20] Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., Gagnon, G. (1999). 'Cyberterror: Prospects and Implications', Defense Technical Information Center, Fort Belvoir, VA.

terrorizmin kibernetik[21].

Ndryshe nga sulmet konvencionale terroriste, terrorizmi kibernetik nuk kërcënon domosdoshmërisht përmes dhunës, njerëzit ose infrastrukturën fizike[22]. Këto sulme mund të jenë operacione që synojnë të prishin ose shkatërrojnë pronën digjitale. Konteksti gjeopolitik në fund të shekullit të 20-të, si dhe fillimi i digjitalizimit dhe debatet rreth "shoqërisë së informacionit", katalizuan më tej konceptin e terrorizmit kibernetik. Menjëherë pas sulmit terrorist të 11 shtatorit në SHBA, një grup hakerash i quajtur Dispatchers njoftoi se do të sulmonte shtetet që mbështesin terroristët. Ky grupim ndërhyri dhe shkatërroi qindra faqe interneti dhe nisi sulme (Distributed Denial-of-Service/DDoS) kundër shteteve të tilla si Irani apo Afganistani, për të treguar kapacitetin ndikues dhe aftësitë e tyre[23]. Tre vjet më vonë, një botim tjetër, *'Terrorism in the Information Age: New Frontiers'*[24] theksoi cenueshmërinë e infrastrukturës kritike ndaj sulmeve dhe demonstroi interesin e terroristëve për të synuar "site" të tilla. Kohët e fundit, koncepti i terrorizmit kibernetik është studiuar gjerësisht akademikë, media, autoritetet qeveritare dhe komuniteti ndërkombëtar, veçanërisht në aspektin e valës së sulmeve 'ransomware' që synojnë ose prekin operatorët kritikë të infrastrukturës, siç ndodhi me qendrat spitalore në Francë dhe Irlandë, apo sistemet e furnizimit me karburantet dhe industria e përpunimit të mishit në SHBA[25]. Këto raste treguan sesi impakti në popullatë mund të tejkalojë shumë shpejt limitet e instrastrukturës kritike.

Pavarësisht kontekstualizimit praktik të terrorizmit kibernetik, sfida mbetet në lidhje me klasifikimin dhe dallimin e këtij akti kriminal nga krimet e tjera kibernetike. Edhe në rastet kur shtetet janë përpjekur ta përfshijnë në legjislacionin e brendshëm terrorizmin kibernetik, nuk janë ofruar dallime të qarta krahasuar me taktikat e tjera terroriste[26]. Ky fakt u theksua edhe nga Asambleja e Përgjithshme e OKB-së në vitin 2021, përmes avancimit të praktikave shtetërore për zbulimin, hetimin dhe ndëshkimin e këtij akti kriminal.

Terrorizmi i mundësuar nga hapësira kibernetike: orientohet nga rastet kur hapësira kibernetike shërben si lehtësues për kryerjen e akteve terroriste, për të theksuar rëndësinë e përhapjes së sulmeve kibernetike nga grupet terroriste. Mjetet për një sulm të tillë mund të prekin komunitete e vendbanime, thjesht, për shkak të sistemeve kibernetike të dobëta, ndaj përgatitja për çdo rast shndërrohet në

[21] Soesanto, S. (2020). 'Cyber Terrorism: Why it exists, Why it doesn't, and Why it Will', Real Instituto Elcano

[22] Denning, D.E. 'A View of Cyberterrorism Five Years Later', Internet Security: Hacking, Counterhacking, and Society. Edited by K. Himma (Sudbury, MA: Jones and Bartlett Publishers, 2007).

[23] Denning, D. (2001). 'Is Cyber-Terror Next?', Social Science Research Council. (Accessed online).

[24] Nicander, L., Ranstorp, M. (2004). 'Terrorism in the Information Age: New frontiers?', Swedish National Defence College.

[25] Boholm, M. (2021). 'Twenty-five years of Cyber Threats in the News: A study of Swedish newspaper coverage (1995-2019)', Journal of Cybersecurity, 7(1), (Accessed 15 November 2021); 'Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment', British Journal of Political Science, pp. 1-19; Soesanto, S. (2020). 'Cyber Terrorism'.

[26] Broeders, D., Cristiano, F., Weggemans, D. (2021). 'Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy', Studies in Conflict and Terrorism, 0, pp. 1-28. (Accessed 15 November 2021); Denning, D.E. (2001). 'Activism, Hacktivism, and Cyberterrorism: The internet as a tool for influencing foreign policy', Networks and Netwars: The Future of Terror, Crime, and Militancy. Edited by J. Arquilla and D. Ronfeldt (Rand Corporation); Flemming, P., Stohl, M. (2001). 'Myths and Realities of Cyberterrorism'

prioritet kombëtar. Përmes rasteve nga kontekste dhe sisteme të ndryshme, ky raport synon të rrisë ndërgjegjësimin për përgatitje paraprake dhe nevojën për plane vendore që parandalojnë sulmet kibernetike terroriste. Rritja dhe pasojat e sulmeve kibernetike – veçanërisht sulmet "*ransomware*" – tregojnë se rreziku rritet nga varësia e shoqërisë dhe ndërvarësia me sistemet e bazuara në hapësirën kibernetike.

Qendra për Studime Strategjike dhe Ndërkombëtare (CSIS) ofron disa ilustrime përmes listës së sulmeve kibernetike që shoqërohen me pasoja të rënda: në 2015, ofruesi i telekomunikacionit TalkTalk raportoi prekjen e të dhënave që zbuloi rreth 157,000 regjistrime të klientëve, i cili u shoqërua me një email "virus" dhe një kërkesë për shpërblim[27]. Në vitin 2017, sulmi "WannaCry" shpërtheu në të gjithë globin dhe shkatërroi pjesë të Shërbimit Shëndetësor Kombëtar të Mbretërisë së Bashkuar (NHS). Në vitin 2021, një sulm dëmtoi dhe nxori jashtë funksionit tubacionet qendrore të furnizimit me karburant në bregun lindor të Amerikës; një tjetër sulm në distancë u përpoq të helmonte furnizimin me ujë të një qyteti në Florida duke rritur sasinë e hidroksidit të natriumit[28], dhe Coop Sweden mbyllën 665 dyqane pasi pikat e shitjes dhe vetë-shërbimit ndaluan së punuari për shkak të infiltrimit në software, dhe bllokimit të shitjeve. Rasti i fundit është vetëm një pjesë e impaktit global që pati kjo industri tek përdoruesit dhe që thekson dimensionin ndërkombëtar të kërcënimit kibernetik. Sipas CSIS, vetëm në muajin janar 2024 u ndërmorën mbi 15 sulme kibernetike ndaj agjencive qeveritare kanadeze, suedeze, australiane; kompanive të mbrojtjes dhe të teknologjisë, ose bizneseve ndërkombëtare, duke pësuar humbje miliona dollarshe[29].

Hapësira kibernetike është përdorur për qëllime të paligjshme nga terroristët; ai mund të shërbejë gjithashtu si një mjet për sulmet terroriste, si dhe një shërbim (mundësues) i drejtpërdrejtë për lehtësimin e këtyre sulmeve. Terrorizmi i nxitur nga hapësira kibernetike ka potencialin të përhapë frikë, të krijojë panik në popullsi ose të detyrojë një qeveri ose organizatë ndërkombëtare të bëjë (ose të heq dorë) nga politika ose veprime institucionale. Numri i shembujve dhe skenarëve të sulmeve kibernetike tregon se si sulmet DDoS, fushatat e *ransomware, phishing,* manipulimi i të dhënave dhe prishja e faqeve të internetit mund të jenë tërheqëse për terroristët.

[27] UK Government (2016). 'National Cyber Security Strategy 2016-2021', p. 20. (Accessed online).

[28] BBC (2021). 'Hacker Tries to Poison *ater Supply of Florida Cty', (8 February). (Accessed online)

[29] Centre for Strategic and International Studies. 'Significant Cyber Incidents'. (Accessed online).

Kjo tendencë në rritje e ka detyruar Departamentin Amerikan të Drejtësisë të theksojë prioritetet dhe rëndësinë e hetimit të ransomware njëlloj si për terrorizmin[30]. Ky perceptim i sulmeve *ransomware*, edhe kur kryhen nga grupe kriminale, tregon gravitetin me të cilin ato shihen dhe ndikimin që mund të kenë. Nëse një sulm kibernetik është në shkallë ndërkombëtare, kombëtare ose lokale; me fokus të përcaktuar (individual, organizativ ose rajonal); ose i përhapur (organike dhe sporadike e bazuar në software ose sisteme etj.), mund të ketë pasoja të rëndësishme që shfaqen në të gjitha nivelet e shoqërisë. "Darkweb", për shembull, ofron anonimitet dhe mundësi për t'u fshehur nga ana e aktorëve keqdashës dhe shërben si një hapësirë diskutimi, koordinimi dhe veprimi ndërmjet tyre. Ai mund të lehtësojë shkëmbimet ndërkombëtare ndërmjet grupeve armiqësore, të mundësojë akses në forma të panumërta të produkteve të paligjshme dhe shërbime kriminale. ISIS dihet se ka hakuar llogaritë e Twitter[31], për shembull, dhe hetime të shumta e operacione kundër terrorizmit kanë treguar përdorimin e enkriptimit nga Al-Kaeda dhe individë të lidhur me ISIS-in, duke komunikuar më shpejt, gjerësisht dhe fshehurazi për të nxitur terrorin në një shkallë më të gjerë[32]. Rekrutimi, radikalizimi, mbledhja e fondeve, shpërndarja e propagandës dhe inkurajimi i dhunës ose mundësimi i sulmeve fizike drejtohen përmes kanaleve online. Në një shembull, 4 website false nga një grup i njohur islamik përdorin kripto-monedhën për të financuar sulmet terroriste.[33]

Kjo qasje kombinohet me shkëmbime të ndërsjella ekspertize dhe trajnimesh kibernetike; platforma të botës së krimit në "darkweb" që kapërcejnë kufijtë; rrjete klandestine; dhe një mikro-ekonomi e ndërtuar mbi kripto-monedha[34]. Ndërmjet vitit 2016-2017, ISIS nisi serinë e parë të suksesshme të sulmeve DDoS, të koordinuara nëpërmjet një hapësirës "darkweb" dhe duke synuar kryesisht infrastrukturën qeveritare. U raportua se ISIS kishte përdorur një shërbim DDoS-for-hire, duke treguar lidhjen midis krimit kibernetik dhe terrorizmit të nxitur nga hapësira kibernetike [35].
Modeli "krimi-si-shërbim" ngre shqetësimin ndaj grupeve terroriste me aftësi të ulëta për blerjen e shërbimeve apo algoritmeve të para-

[30] Bing, C. (2021). 'Exclusive: U.S. to Give Ransom*are Hacks Similar Priority as Terrorism', Reuters. (Accessed online).

[31] Hymas, C. (2019). 'ISIL Terrorists Hack Ordinary Peoples' Dormant Twitter Accounts', The Telegraph (18 November). (Accessed online).

[32] UNOCT (2021). 'Algorithms and Terrorism: The malicious use of artificial intelligence for terrorist purposes. A Joint Report by UNICRI and UNCCT', pp. 17-18. (Accessed online).

[33] Greenberg, A. (2020). 'ISIS Allegedly Ran a Covid-19 PPE Scam Site'. (Accessed online).

[34] US Department of Justice (2012). 'Assistant Attorney General for National Security Lisa Monaco Speaks at the "2012 Cybercrime Conference"'. (Accessed online).

[35] Flashpoint (2017). 'Cyber Jihadists Dabble in DDoS: Assessing the threat'. (Accessed online).

ndërtuara për qëllimet e tyre kriminale. Qendra Evropiane e Krimit Kibernetik tani ofron ekspertizë për hetime ku krimi kibernetik dhe terrorizmi ndërlidhen me njëra-tjetrën[36]. Që nga viti 2017, divizioni për hakerim i ISIS ka pretenduar (shënim: sfidat në vlerësimin e besueshmërisë së pretendimeve janë një pengesë tjetër për të kuptuar origjinën e sulmeve kibernetike) përgjegjësinë për sulmet që prishën shërbimet online[37] dhe Europol ka raportuar thirrje të tjera nga grupet terroriste për sulme kibernetike kundër objektivëve të ndjeshëm[38].

[36] Europol (2021). 'European Union Terrorism Situation and Trend report', p. 105. (Accessed online).
[37] UNOCT (2021). 'Algorithms and Terrorism', p. 27. (Accessed online).
[38] Europol (2021). 'European Union Terrorism Situation and Trend report', p. 59. (Accessed online).

Haktivizmi politik. konsiderohet si një lloj terrorizmi kibernetik ose hakerimi, sidomos nga shtete të caktuara nën maskën e goditjes së fënomeneve politike. Disa nga përkufizimet më të përhapura që ndihmojnë për të kuptuar fenomenin janë këto:

- "përdorimi jo i dhunshëm i mjeteve dixhitale të paligjshme ose ligjërisht të paqarta në ndjekje të qëllimeve politike" (Samuel, 2004)
- "Një kombinim i protestës politike me bazë hakerimin kompjuterik" (Jordan dhe Taylor, 2004)
- "Një veprim i motivuar politikisht, në internet, ose një fushatë komjuterike e ndërmarrë nga një aktor joshtetëror në shenjë hakmarrjeje për të shprehur mosmiratimin ose për të tërhequr vëmendjen ndaj një çështjeje politike" (Vegh, 2003)

Haktivizmi - si një përdorim i motivuar politikisht i aftësive hakeruese, të ndërmarra nga aktorë anonimë joqeveritarë, për të përhapur fjalën, për të tërhequr vëmendjen për një çështje dhe për të shkaktuar ndryshim. Këto janë pikat kyçe që ndihmojnë për të dalluar haktivizmin nga hakerimi, terrorizmi kibernetik dhe aktivizmi online. Për të siguruar një kuptim më të mirë se çfarë ndikimi politik mund të ushtrohet nga haktivistët, së pari duhet të studiojmë stimujt që qëndrojnë pas aktiviteteve haktiviste.

2. Cenueshmëria dhe ndërvarësia

2.1. Infrastruktura kritike e informacionit

Sulmet kibernetike në infrastrukturën kritike mund të shkaktojnë efekte dytësore dhe terciare zinxhir që, në disa raste, shkaktojnë më shumë dëme kolaterale sesa vetë sulmi. Në referim të kuadrit tonë rregullator, me "infrastrukturë kritike të informacionit" kuptohet tërësia e rrjeteve dhe sistemeve të informacionit, të zotëruara nga një autoritet publik ose privat, që ofrojnë shërbime, cenimi apo shkatërrimi i të cilave do të kishte impakt serioz në shëndetin, sigurinë, mirëqenien ekonomike të qytetarëve dhe funksionimin efektiv të ekonomisë në Republikën e Shqipërisë. Për të ilustruar me disa shembuj mbi impaktin dhe efektet zinxhir të sulmeve kibernetike përmendim rastin e Shqipërisë, në mars 2021, kur sulmi kibernetik që synoi paralizimin e shërbimeve publike dhe fshirjen e plotë të informacioneve nga databaza shtetërore; solli si pasojë publikimin e të dhënave personale të qytetarëve dhe zyrtarëve shtetërorë. Në maj 2021, fushata e ransomware kundër kompanisë së naftës dhe gazit "Colonial Pipeline" në SHBA goditi sistemet e IT-së të biznesit dhe fatmirësisht jo fluksin e tubacionit, presionin dhe metrika të tjera. Megjithatë, meqë informacioni mbi pagesat, porositë e blerjes dhe inventari nuk u prekën, kompania u detyrua të përdorë disa sisteme jashtë linje, duke përfshirë tubacionet kryesore. Ky vendim bëri jehonë në ekosistemin amerikan dhe çoi në ndërprerje të shpërndarjes, panik dhe mungesën e furnizimit në shumë pika karburanti [39]. Kërkesa e shoqërive për karburant do të thotë se një destabilizim i tillë mund të ketë efekte të gjera në funksionimin e qyteteve, zinxhirin e furnizimit, ekonominë dhe madje edhe në tregjet ndërkombëtare.

Efekte të tjera pati një fushatë ransomware në Spitalin Universitar të Düsseldorf-it (Gjermani) në shtator 2020. Ransomware infektoi sistemin kompjuterik që përdorej për të koordinuar turnet e mjekëve, operacionet kirurgjikale, trajtimin mjekësor dhe menaxhimin e pacientëve sipas shtretërve. Duke qenë se këto të dhëna u bllokuan, spitalit iu desh të anullonte mijëra operacione, të kufizonte në mënyrë drastike kapacitetin e tij për të trajtuar pacientët dhe të ndalonte të gjitha pranimet e reja. Mbyllja efektive e spitalit solli raportimin e 2 humbje jetësh (një grua 78-vjeçare me aneurizëm të aortës, në pritje të operimit; dhe një rast vetëvrasjeje në mungesë të prezencës së mjekut roje). Ngjarjet u hetuan nga prokuria, e cila argumentoi se vdekja e parë ndodhi për shkak të gjendjes shëndetësore dhe

> "Infrastruktura kibernetike mbështet infrastrukturën kritike si termocentralet, hidrocentralet dhe sistemet e ujësjellës kanalizimeve, qendrat shëndetësore dhe spitalore, sistemet e telekomunikacionit, rafineritë e naftës dhe gazit dhe rrjetin e transportit dhe rrugët kombëtare."
>
> *Agjencia e Sigurisë Kibernetike dhe Sigurisë së Infrastrukturës (SHBA) "Korniza e Planifikimit të Qëndrueshmërisë së Infrastrukturës"*

[39] Krauss, C. et al. (2021). 'Gas Pipeline Hack Leads to Panic Buying in the South-east', The New York Times (11 May). (Accessed online).

jo nga sulmi i *ransomware*. Kryeprokurori publik përgjegjës për hetimin, megjithatë, vuri në dukje rastin si "një shenjë paralajmëruese për ata që menaxhojnë infrastrukturën kritike" se dështimi për të mbrojtur në mënyrë adekuate këto sisteme "mund të përfundojë në rezultate fatale" [40].

Në të vërtetë, sulmet kibernetike ndaj kujdesit shëndetësor mund të kenë pasoja serioze, siç tregohet nga sulmi WannaCry që ndikoi në sistemin shëndetësor në Mbretërinë e Bashkuar.

2.2. Rast studimor - Sulmi WannaCry ransomware

Të premten, më 12 maj 2017, një sulm global ransomware, i njohur si WannaCry, preku një gamë të gjerë qytetesh dhe sektorësh. WannaCry infektoi kompjutera që ekzekutonin disa versione të sistemit operativ Microsoft Windows duke shfrytëzuar një dobësi specifike të Windows, duke enkriptuar të dhënat dhe duke kërkuar pagesa shpërblimi në kriptomonedhën Bitcoin. Brenda një dite, Europol raportoi infektimin e më shumë se 250,000 kompjutera në të paktën 150 qytete[41], duke përfshirë sistemet e administratës qendrore së sistemit shëndetësor në Mbretërinë e Bashkuar. Sulmi preku të paktën 80 nga 236 fonde sigurimesh për mbulimin financiar të shërbimeve shëndetësore (truste) në sistemin shëndetësor në të gjithë Anglinë (a) si pasojë e infektimit të disa kompjuterave nga ransomware (b) ose si pasojë e fikjes se pajisjeve si masë paraprake. Rreth 603 qendra të kujdesit parësor dhe agjenci e kabinete shëndetësore u infektuan, duke vënë në rrezik 595 ndërhyrje kirurgjikale. Firma e sigurisë kibernetike Avast e identifikoi WannaCry si një nga sulmet kibernetike më të gjera dhe më të dëmshme në histori. Përveçse është sulmi më i madh kibernetik që ka prekur sistemin shëndetësor kombëtar në Mbretërinë e Bashkuar deri më sot, ndikimi i WannaCry u regjistrua deri në Rusi, Ukrainë dhe Tajvan, në universitetet kineze, tek firmat spanjolle Telefónica dhe firmat globale si FedEx, Nissan dhe Renault[42].

- **Përgjigjet e Sistemit Kombëtar Shëndetësor britanik**

Shërbimi Dixhital CareCERT i Sistemit Kombëtar Shëndetësor njoftoi Departamentin e Shëndetësisë rreth orës 13.00 më 12 maj 2017, pas raportimeve të shumta nga trustet e NHS. Sulmi u përcaktua si një incident i madh ndaj sistemit kombëtar shëndetësor (NHS) në orën 16.00, duke garantuar zbatimin e një strukture komandimi dhe kontrolli kombëtar sipas planeve ekzistuese të Emergjencave, Gatishmërisë, Qëndrueshmërisë dhe Reagimit. NHS e Londrës veproi si pika e vetme e koordinimit për menaxhimin e incidenteve me mbështetjen e Shërbimit Digjital dhe Shërbimeve Mbështetëse. ora 17:00, qendrat rajonale të koordinimit të incidenteve në NHS filluan të kërkonin konfirmime nga organizatat lokale të NHS se veprimet po ndërmerreshin në përputhje me komunikimet CareCERT. Organizatat lokale punuan për të zgjidhur dhe parandaluar sulmin kibernetik ku ishte e mundur. Më vonë në mbrëmjen e 12 majit 2017, një ekspert zbuloi versionin "kill switch" që ndaloi përhapjen e mëtejshme të *malware*. Shërbimi Digjital u shkroi të gjitha trusteve më 14 maj 2017 për të

[40] Ralston, W, (2020). 'The Untold Story of a Cyberattack, a Hospital and a Dying Woman', Wired (Accessed online).

[41] CNBC (2017). 'Unprecedented Cyber-Attack Hits 200,000 in At Least 150 Countries, and the Threat Is Escalating'. (Accessed online).

[42] Larson, S. (2017). 'Massive cyberattack targeting 99 countries causes sweeping havoc'. CNN. (Accessed online).

mos kryer asnjë pagesë si shpërblim për rikthimin e të dhënave.[43]

Përgjigja e NHS ndaj sulmit u formulua nga tre faza:

- Mbrojtja e kanaleve për urgjencat shëndetësore;
- Qëndrueshmëria dhe operavionaliteti i kujdesit parësor;
- Riparimi i dëmeve, veprime më të gjera të sistemit dhe aplikimi i përditësimit antivirus.

Në përputhje me planet ekzistuese për reagimin ndaj incidenteve të mëdha, NHS fillimisht u përqendrua në mirëmbajtjen e shërbimeve të urgjencës. Koha e sulmit, duke filluar të premten, rezultoi në ndërprerje minimale të shërbimeve të kujdesit parësor, të cilat zakonisht mbyllen gjatë fundjavës. Sulmi WannaCry ndërpreu shërbimet e NHS në të gjithë vendin deri më 19 maj 2017, kur incidenti kombëtar u bllokua. Gjatë kësaj periudhe, Departamenti i Shëndetësisë dhe NHS Angli punuan me NHS Digjital, Qendrën Kombëtare të Sigurisë Kibernetike, Agjencinë Kombëtare të Krimit dhe të tjerë për t›iu përgjigjur sulmit dhe për të mbështetur shërbimet e NHS në ofrimin e kujdesit për pacientët. NHS Angli zbatoi planet e incidenteve të mëdha dhe koordinoi reagimin përmes të njëjtave ekipe dhe struktura që do të merreshin me çdo incident tjetër të madh kombëtar. Kjo ishte një kornizë e fortë përmes së cilës mund të menaxhohej incidenti.

➢ Impakti dhe mësimet e nxjerra

Kujdesi shëndetësor është një mjedis kompleks me shumë sisteme të lidhura. NHS iu përgjigj në mënyrë efektive këtij incidenti madhor, pa raportime për dëme ose humbje jetësh të pacientëve, pa cënim të të dhënave të pacientëve apo vjedhje të të dhënave. Është vlerësuar nga NHS Angli se 1% e aktivitetit të NHS u ndikua drejtpërdrejt nga sulmi WannaCry gjatë javës së sulmit. Nga 236 fonde sigurimesh për mbulimin financiar të shërbimeve shëndetësore (truste) në të gjithë Anglinë, 80 u prekën rëndë, duke prekur shërbimet pavarësisht nëse sistemi nuk ishte e infektuar nga virusi (për shembull, nëse u përdorën serverat e postës elektronike ose lidhjet e rrjetit jashtë linje). Disa pajisje mjekësore kritike po përdornin ende software Microsoft Windows 7 ose XP të ofruar nga palë të treta; këto pajisje u prekën, duke përfshirë, për shembull, skanerat e rezonancës magnetike (MRI) dhe pajisjet e analizave të gjakut. Rezultati ishte se

[43] National Audit Office. 'Investigation: WannaCry cyber-attack and the NHS'. (Accessed online).

pajisjet diagnostikuese u bënë të papërdorshme pasi software funksiononte në një pajisje të infektuar dhe duhej të rregullohej ose karantinohej. NHS Angli identifikoi se 6,912 takime ishin anuluar dhe rreth 19,000 takime referimi u prekën (fshinë, ndryshuan). Nuk dihet se sa konsulta mjekësore janë anuluar, apo sa ambulanca dhe pacientë janë devijuar nga pesë departamentet e urgjencës që nuk kanë mundur të trajtojnë disa pacientë. NHS Angli thotë se është e pamundur të llogaritet me siguri ndikimi financiar i sulmit WannaCry. Një vlerësim i përgjithshëm flet për 92 milion £, duke përfshirë shërbimin dhe kostot e IT nga sulmi.[44]

Pas sulmit kibernetik të WannaCry, u ndërmor një seri takimesh informuese ndërmjet agjencive, vlerësime të brendshme organizative. Bordi Udhëheqës i Sigurisë së të Dhënave të Departamentit të Shëndetësisë ngarkoi gjithashtu Zyrtarin e Lartë të Informimit për sistemin e kujdesit shëndetësor dhe social në Angli për të kryer një rishikim gjithëpërfshirës të sulmit. Zyra Kombëtare e Auditimit hetoi gjithashtu efektin që kishte sulmi WannaCry në NHS në Angli.

Disa nga rekomandimet kryesore janë paraqitur më poshtë:

Vlerësimi i Zyrtarit të Lartë të Informimit arriti në përfundimin se sulmi theksoi dobësitë brenda NHS në Angli. Ai ekspozoi nevojën për të përmirësuar të gjithë sistemin NHS, duke përfshirë disiplinën dhe përgjegjshmërinë rreth sigurisë kibernetike në nivel të lartë drejtues dhe bordi, dhe rëndësinë e përgjigjes së shpejtë dhe efektive të sistemeve kur bëhen përditësimet e reja të sigurisë. Vlerësimi identifikoi investime të ulëta për sigurinë e rrjetit dhe software të përditësuar.

Një nga mësimet kryesore ishte nevoja për qartësi mbi udhëheqjen dhe përgjegjësinë për çdo incident të ardhshëm të sigurisë kibernetike. Kjo u trajtua përmes zhvillimit të një "udhëzuesi kibernetik" për të përshkruar qasjen dhe veprimet që duhen ndërmarrë nga NHS Angli, NHS Improvement dhe NHS Digital në rast të një sulmi kibernetik.
Në parim, Departamenti i Shëndetësisë do të drejtonte përgjigjen e sistemit. Vlerësimi rekomandoi zhvillimin e planeve të vazhdimësisë së biznesit, reagimit kibernetik dhe rikuperimit të katastrofave të organizatave lokale për të përfshirë detajet e nevojshme rreth incidenteve kibernetike. Kjo përfshiu vlerësimin e ndikimit të humbjes së shërbimeve në pjesë të tjera të sistemit të kujdesit shëndetësor dhe social.[45] Vlerësimi gjithashtu theksoi se planet duhet të testoheshin rregullisht nëpër organizata dhe partnerë lokalë, me mbikëqyrje në nivel bordi. Shërbimi Shëndetësor Digjital përgatiti një Test Reagimi ndaj Incidentit Kibernetik[46] për të mbështetur organizatat lokale në testimin e reagimit ndaj incidenteve në kujdesin shëndetësor dhe social.

Nevoja për të ndërtuar fleksibilitetin e organizatave lokale u nxit më tej nga rekomandimet për zhvillimin e ofruesve dhe shërbimeve digjitale; mbrojtjen e pacientit; heqjen ose izolimin e sistemeve të pambështetura dhe versioneve të pambrojtura të software; investimet në infrastrukturë.

Rekomandimet për të përmirësuar infrastrukturën dhe planifikimin lokal u shoqëruan me zhvillimin menaxherial të qeverisjes. Kjo do të thoshte se të gjitha organizatave të NHS tani iu kërkua të caktonin një drejtor ekzekutiv si drejtues i sigurisë së të dhënave; Rreziqet e sigurisë kibernetike duhet të rishikoheshin rregullisht nga bordi; dhe duhet të merreshin masat e duhura si kundërpërgjigje për të zbutur

[44] UK Government. (2018) 'Securing Cyber Resilience in Health and Care: October 2018 update'. (Accessed online).

[45] NHS England (2018). 'Lessons Learned Revieë of the WannaCry Ransomware Cyber Attack'. (Accessed online).

[46] NHS Digital. Cyber Incident Response Exercise (CIRE). (Accessed online).

ose zvogëluar ndikimet e një sulmi tjetër ndërkohë që shërbimi ishte gjatë restaurimit.[47]

U bënë përpjekje për transformimin dixhital të gjithë shërbimit NHS, duke përfshirë përgjegjësitë për ofrimin e drejtimit strategjik dhe monitorimin e sigurisë kibernetike. Një punë e rëndësishme u ndërmor gjithashtu për të zhvilluar sistemin shëndetësor digjital CareCERT, i cili tani ka evoluar në sistemin "*Respond to an NHS cyber alert*", i cili lejon dërgimin e mesazheve tek organizatat shëndetësore dhe ato të kujdesit social, siguron konfirmimin e marrjes dhe merr përditësime mbi progresin me punën e rehabilitimit.

Është e pashmangshme që sistemet shëndetësore dhe të kujdesit social të përballen me sulme në të ardhmen. Kjo kërkon vigjilencë dhe një proces vlerësimi dhe menaxhimi të këtyre kërcënimeve.
Si të tilla, DH dhe NHS vazhdojnë të investojnë në sigurinë kibernetike në të gjitha nivelet. Ndërsa peizazhi i kërcënimit evoluon vazhdimisht dhe sistemet dixhitale bëhen gjithnjë e më të fokusuara në ofrimin e kujdesit shëndetësor për publikun, ka pasur përmirësime në tre fusha kryesore: monitorimi kibernetik, inteligjenca ndaj kërcënimeve dhe reagimi ndaj incidenteve; mbështetje dhe udhëzime për organizatat lokale; plus trajnimin kibernetik, ndërgjegjësimin dhe angazhimin me praktikat më të mira të sigurisë kibernetike.

[47] NHS England (2018). 'Lessons Learned Revie* of the *annaCry Ransom*are Cyber Attack'. (Accessed online).

2.3. Sulmet kibernetike me të cilat është përballur Shqipëria

Qasja e Shqipërisë ndaj sigurisë kibernetike ndahet në dy periudha:

1. rrjedhjet e të dhënave para vitit 2022[48];
2. rrjedhjet e të dhënave dhe sulmeve kibernetike pas vitit 2022.

Në vitin 2022, rreth 1 milion sulme kibernetike shënjestruan Shqipërinë, ku 80% e tyre e kishin origjinën nga Irani[49]. Sulmi ndaj infrastrukturës kritike të Shqipërisë paralizoi vendin, i cili sapo kishte përfunduar tranzicionin e ofrimit të një numri të konsiderueshëm të shërbimeve publike vetëm online. Qëllimi dhe synimi i sulmit ishte tërësisht brenda përkufizimit të termit të veprave penale në kuadër të terrorizmit. Grupi i vetëquajtur HomeLandJustice, i kërkonte shtetit shqitpar që të largonte nga Shqipëria anëtarët e organizatës MEK, e cila është në opozitë me regjimin aktual në Iran. Ky pretendim ngrihej mbi argumentin se MEK kryente veprime të paligjshme ndaj Iranit dhe për këtë qëllim, Shqipëria, duke qenë se kishte garantuar qëndrimin e tyre, mbante përgjegjësi që jo vetëm strehonte një grup të konsideruar terrorist nga Irani por dhe lejonte hapësirën e saj kibernetike për kryerjen e akteve terroriste online.
Pas sulmit, një hetim i përbashkët i FBI dhe Microsoft zbuloi se hakerët e HomeLand Justice ishin infiltruar në sistem 9 muaj para sulmit[50]. Kjo gjetje ishte shqetësuese për sa i përket vulnerabilitetit të infrastrukturave kritike dhe të rëndësishme në vend.

Rrjedhjet e të dhënave personale e zhvendosën fokusin e qeverisë në nevojën kritike për masa më të forta të sigurisë kibernetike, pavarësisht se kur hedhim një vështrim mbrapa për mënyrën se si Qeveria shqiptare trajtoi sulmet kibernetike dhe rrjedhjen e të dhënave, vërejmë se ska asnjë element të ri apo ndryshim në metodologjinë e përdorur. Qasja më së

[48] Të dhënat e rreth 910,000 shqiptarëve në listën e Patronazhistëve; të dhënat personale dhe pagat për 637,138 qytetarë shqiptarë, dhe informacioni privat për targat e makinave dhe numrat e telefonit për 650,000 shqiptarë u zbuluan dhe u bënë pjesë e domenit publik.

[49] https://kohajone.com/flet-mbreti-i-sigurise-kibernetike-shqiptare-igli-tafa/

[50] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a

shumti ka qenë e fokusuar se “i kujt është faji” sesa “masat që duhen marrë për të evituar përsëritjen në të ardhmen e afërt” apo kryerjen e analizave mbi impaktin social që kanë pasur këto sulme dhe dëmet e drejtpërdrejta që ju janë shkaktuar qytetarëve, paralelisht me analizën e dëmeve të shkaktuara në infrastrukturat e informacionit, infrastrukturat kritike apo rrjeteve te komunikimit. Këto lloj analizash zakonisht duhet të kryhen nga të gjithë aktorët si ata institucionalë, publikë, jo-publikë, OJF-të, ekspertët e fushës së TIK, përfaqësues të akademisë apo dhe ekspertët ndërkombëtarë në bashkëpunim me njëri-tjetrin në mënyrë që të ndërtohen plane për përgjigje të koordinuar ndaj sulmeve të mëdha kibernetike dhe plane përgatitjeje multidimensionale me hapa konkrete me qëllim mitigimin e rasteve të sulmeve kibernetike apo rrjedhjes së informacioneve konfidenciale, sensitive apo sekret shtetëror.

Në kohën kur ndodhi sulmi kibernetik, Shqipëria po kalonte në një model të qeverisjes tërësisht elektronike duke ofruar shërbimet publike vetëm online, nëpërmjet sistemeve kompjuterike të informacionit[51]. Nga ana tjetër, Strategjia Kombëtare e Sigurisë Kibernetike 2020-2025 pranonte mungesën e mjeteve të nevojshme të Qeverisë për të siguruar inteligjencë kibernetike për veprimtarinë e organeve ligjzbatuese dhe mungesën e burimeve njerëzore me aftësitë dhe kualifikimet e duhura për të adresuar sfidat e sigurisë kibernetike. Edhe pse synimi ishte “garantimi i sigurisë kibernetike në nivel kombëtar përmes mbrojtjes së infrastrukturës së informacionit”, realiteti provoi të kundërtën.

Sulmet kibernetike e gjetën Qeverinë duke promovuar arritjet e qeverisjes dixhitale dhe kërkesës së llogarisë së publikut lidhur me këto sulme, Qeveria ju përgjigj duke parashtruar disa argumente ndër të cilat ishin që portali unik qeveritar e-Albania nuk ruan të dhëna; edhe Qeveri të tjera më të forta në aspektin e sigurisë kibernetike janë sulmuar nga sulme të tilla apo si dhe, ne bëmë më të mirën që kishim mundësi.

Nëse i referohemi në mënyrë të përmbledhur sulmeve kibernetike të kryera në Shqipëri në një hark kohor prej pothuajse dy vitesh, evidentohet se në shumicën e rasteve të dëmtuarit kryesorë janë qytetarët, qofshin këta të veshur me pozicione publike apo qytetarë të thjeshtë, përdorues shërbimesh publike dhe jo-publike.

[51] Aktualisht është miratuar një ligj i ri për qeverisjen elektronike. Ligji Nr. 43/2023 “Për Qeverisjen Elektronike”.

- Në datë 15 Korrik 2022[52], hacker-ët shkaktuan ndërprerje të përkohshme në faqet e internetit të Zyrës së Kryeministrit të Shqipërisë dhe Parlamentit, si dhe në portalin unik qeveritar e-Albania i përdorur për të aksesuar dhe përdorur shërbimet publike.

- Në shtator 2022, hackerët iranianë synuan sistemet kompjuterike shqiptare, duke detyruar zyrtarët shqiptarë të mbyllin përkohësisht Sistemin e Përgjithshëm të Menaxhimit të Informacionit, një shërbim i përdorur për të ndjekur individët që hyjnë dhe dalin nga Shqipëria. Ky sulm u shoqërua ngushtë me vendimin e Shqipërisë për të shkëputur lidhjet diplomatike me Iranin, siç edhe Kryeministri i Shqipërisë, Edi Rama, njoftoi në një deklaratë video[53] se një seri sulmesh shkatërruese në infrastrukturën dixhitale kritike të vendit në fillim të verës ishin atribuar Republikës Islamike të Iranit (IRI), dhe si rezultat, qeveria po ndërpriste marrëdhëniet diplomatike me Teheranin si dhe me sanksionet amerikane dhe dënimin e NATO-s për një sulm kibernetik iranian kundër Shqipërisë në korrik. Në sulmin e korrikut, aktorët iranianë vendosën ransomware në rrjetet e Qeverisë Shqiptare që shkatërroi të dhëna dhe shkaktoi ndërprerje në shërbimet qeveritare.

- Më 19 shtator 2022, dymbëdhjetë ditë pasi Shqipëria ndërpreu marrëdhëniet diplomatike me Republikën Islamike të Iranit, HomeLand Justice publikoi në kanalin e tyre të Telegramit një dokument prej 47 faqesh të të dhënave të vjedhura. Dosja përmbante informacion personal identifikues si dhe regjistrime të kalimeve kufitare të ish-drejtorit të përgjithshëm të Policisë së Shtetit të Shqipërisë, Gledis Nano, dhe familjes së tij.

- Më pak se një muaj më vonë, më 3 tetor, i njëjti grup HomeLand Justice publikoi një dokument tjetër voluminoz, këtë herë me madhësi mbi 1.7 gigabajt, i cili ekspozonte 300 identitete të personave të dyshuar për vepra penale në Shqipëri. Kjo shpërndarje të dhënash sugjeron fort se hakerët kishin hyrë në sistemin e avancuar të komunikimit të policisë së Shqipërisë të quajtur Memex[54], duke ngritur shqetësime të forta për masat e mbrojtjes së të dhënave kombëtare.

- Pas tyre, vazhduan rrjedhje periodike të informacionit. Më 19 tetor, hakerët publikuan një dosje lidhur me drejtorin e inteligjencës shqiptare, Helidon Bendo, që përmbante të dhëna prej 17 vjetësh (2005-2022) nga Sistemi i Përgjithshëm i Menaxhimit të Informacionit (TIMS), duke ekspozuar përsëri hyrjet dhe daljet e regjistruara në kufirin shtetëror.

- Më 2 nëntor, grupi rriti rrezikun sërish duke publikuar identitetet dhe detajet personale të 600 oficerëve të inteligjencës shqiptare, duke përfshirë emrat, email-et dhe numrat e telefonit.

---

[52] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[53] https://www.kryeministria.al/en/newsroom/videomesazh-i-kryeministrit-edi-rama-lidhur-me-vendimin-e-qeverise-shqiptare-si-kunderpergjigje-ndaj-aktit-te-sulmit-te-rende-kibernetik-ndaj-infrastruktures-digjitale-te-qeverise-se-republikes-se-s/

[54] https://albanianpost.com/bie-sistemi-me-i-sofistikuar-i-komunikimit-policor-homeland-justice-vijon-publikimet-e-materialeve/

- Gjashtë ditë më pas, HomeLand Justice publikoi një video të një operacioni të inteligjencës shqiptare në bashkëpunim me Policinë e Shtetit, që përfshinte pamje të ish-shefit të policisë Nano.

Siç u bë e qartë nga deklarata e kryeministrit shqiptar më 7 shtator, sulmet kibernetike dhe rrjedhjet e informacionit në fillim të vjeshtës nuk ishin hera e parë që grupi i hakera-ve HomeLand Justice bëhej i njohur në vend. Më parë, hakerët e lidhur me këtë grup kishin vjedhur korrespondencën e shkëmbyer ndërmjet ministrive, ambasadave, dhe madje edhe email-at e Kryeministrit me qytetarë shqiptarë. Çdo herë, grupi e bënte këtë të ditur në Telegram. Dhe më 15 korrik, sulmuesit kibernetik njoftuan në Twitter se kishte në plan të kryente sulme kibernetike kundër Agjencisë Kombëtare për Shoqërinë e Informacionit të Shqipërisë (AKSHI) siç edhe ndodhi.

- Në 25 dhjetor 2023[55], grupi HomeLand Justice arriti të depërtojë tek të dhënat e kompanisë së telekomunikacionit 'One', kompanisë ajrore 'Air Albania' si dhe sulmuan faqen zyrtare të Kuvendit të Shqipërisë.

- Më datë 1 shkurt 2024[56], Instituti i Statistikave është përballur me një sulm kibernetik nga grupi HomeLand Justice që synonte infrastrukturën e tij teknologjike dhe që ka shkaktuar dëme të konsiderueshme në të dhëna.

Nga një vlerësim i riskut për rastin e mësipërm mund të thuhet se:

Shqipëria mund të konsiderohet "hotspot" i krimeve kibernetike me natyrë terroriste: *Shqipëria aktualisht është subjekt i sulmeve kibernetike me natyrë terroriste por mund të rrezikoj të jetë një territor i cili mund të përdoret nga organizata të ndryshme për të kryer veprime terroriste kibernetike ndaj shteteve të tjera.*

Rritja e sulmeve të ngjashme: *Ky sulm mund të shërbejë si shembull për grupet e tjera terroriste të cilat mund të dëshirojnë të ndjekin shembullin dhe të kryejnë sulme të ngjashme në të ardhmen. Kjo rrit mundësinë e përhapjes së sulmeve të këtij lloji dhe përdorimin e taktikave të ngjashme të dëmshme në Shqipëri.*

Rritja e tensioneve ndërkombëtare: *Sulmet kibernetike të tilla kanë çuar në prishjen e marrëdhënieve ndërkombëtare midis vendeve dhe të çojnë në tensione të mëtejshme diplomatike dhe politike edhe me shtete të tjera jo miqësore me Shqipërinë siç është dhe rasti i Rusisë.*

Rënia e besimit publik në sigurinë kibernetike: *Sulmet kibernetike të tilla mund të shkaktojnë një rënie të besimit publik në sigurinë kibernetike dhe në aftësinë e qeverisë për të mbrojtur infrastrukturën kritike nga këto rreziqe.*

[55] https://boldnews.al/2023/12/25/one-albania-nen-kthetrat-e-homeland-justice-hakerat-sulmojne-kompanine-celulare/
[56] https://cesk.gov.al/deklarate/

Gatishmëria për t'iu përgjigjur sulmeve kibernetike duhet të jetë proporcionale me rrezikun, shkallën dhe llojet e shërbimeve që ofrohen

Një fushatë ransomware që synonte rrjetin ICT të transportit publik të Torontos në tetor 2021 shkaktoi mbylljen e sistemit të brendshëm të postës elektronike. Rezervimet në internet u bllokuan dhe sistemi i komunikimit me operatorët u fshi[57]. Operatorët e automjeteve kaluan në radio për të komunikuar me Qendrën e Kontrollit dhe udhëtarët u nxitën të bënin rezervime me telefon. Përgjigja shmangu ndërprerje të rëndësishme të shërbimit dhe nënvizoi rëndësinë e planifikimit të lidhjeve të qëndrueshme të komunikimit. Megjithatë, incidenti rezultoi në humbjen e mundshme të informacionit personal të 25,000 punonjësve aktualë dhe të mëparshëm.[58] Në mungesë të masave të reagimit elastik, një sulm i tillë mund të përballet me një rrjet transporti me sfida të vështira logjistike dhe operacionale. Nga kjo rrjedh se gatishmëria për t'iu përgjigjur sulmeve kibernetike duhet të jetë proporcionale me rrezikun, shkallën dhe llojet e shërbimeve që ofrohen.

Një sulm brenda infrastrukturës së mundësuar nga hapësira kibernetike mund të ketë efekte të rëndësishme "zinxhir". Sikur të marrim në konsideratë se si transporti (ajror, detar dhe ujor, hekurudhor dhe rrugor), stacionet e energjisë ((elektrike dhe bërthamore), impiantet e trajtimit të ujit dhe ujërave të zeza, sistemet e ashensorëve dhe shkallëve lëvizëse, semaforët, sistemet e gazit apo fibrat e telekomunikimit në distanca të gjata janë kryesisht të automatizuara. Ndërsa kalojmë në makina pa shofer, kamionë, autobusë dhe shtëpi inteligjente ose ndërtesa plotësisht të automatizuara me sisteme ngrohjeje, ajrimi, ajri të kondicionuar, ndriçimi dhe hidraulik, sipërfaqja e sulmit do të rritet. Ndërsa infrastruktura kritike bëhet gjithnjë e më dixhitale dhe e ndërlidhur, nevoja për t'u siguruar që ajo është e mbrojtur nga e ardhmja bëhet më urgjente.

Komunikimet – veçanërisht komunikimet satelitore – janë bërë thelbësore për komunikimin, pozicionimin gjeohapësinor, monitorimin e mjedisit, lidhjet e të dhënave dhe mbrojtjen, gjë që ngre shqetësime në lidhje me cënueshmërinë e saj ndaj kërcënimeve të tilla si sulmet kibernetike".[59]

Shërbimet bazë për komunitetin

Aktorët armiqësorë duke përfshirë terroristët mund të përdorin vjedhjen e të dhënave dhe grumbullimin e të dhënave, për shembull, për të studiuar, planifikuar dhe mbështetur sulmet e jetës reale (fizike). Rasti në vijim është identifikuar për të treguar se cenimi i shërbimeve komunitare mund të krijojë efekt zinxhir që sjell impakt të gjerë social.
Në rastin e hakerimit të të dhënave 10-vjeçare për rreth 200 punonjës policie, qendra trajnimi, struktura mbështetëse etj., publikimi i këtyre të dhënave në mesin e vitit 2020 nxiti rreziqe specifike të haktivizmit politik. Pas trazirave dhe protestave në shumë qytete të SHBA për vrasjen e George Floyd, DDoSecrets publikoi 270 GB të dhëna, të njohura si "BlueLeaks"

[57] CBC (2021). 'Toronto Transit System Hit by Ransom*are Attack, TTC Says No Significant Disruptions', The Canadian Press (29 October). (Accessed online); CBC (2021). 'TTC CEO Apologizes in the *ake of Ransom*are Attack', CBC Ne*s (5 November). (Accessed online).
[58] *arrick, J. (2017). 'Use of *eaponized Drones by ISIS Spurs Terrorism Fears', *ashington Post. (Accessed online).

[59] Pescaroli, G. et al (2018). 'Increasing Resilience to Cascading Events: The M.OR.D.OR. scenario', Safety Science 110(C), Elsevier, p. 134. (Accessed online).

në qershor 2020.[60] Të dhënat dolën nga «hakerimi më i madh i publikuar i agjencive amerikane ligjzbatuese dhe ofruan informacione të detajuara të agjencive shtetërore, lokale dhe federale të ngarkuara me mbrojtjen e publikut, duke përfshirë përgjigjen e qeverisë ndaj Covid-19 dhe protestave "BlackLiveMatters". Edhe pse DDoSecrets fshiu afërsisht 50 GB të dhëna sensitive në lidhje me viktimat e krimit, fëmijët, kujdesin shëndetësor dhe shoqatat e veteranëve, mendohet se ka ende te dhëna të tjera që janë fshirë përfundimisht. Të përfshira në miliona skedarë janë të dhënat personale të më shumë se 700,000 punonjësish të agjencive ligjzbatuese në SHBA, historitë e fjalëkalimeve, faturat, emrat e informatorëve, hartat e detajuara të incidentit, videot dhe skedarët audio, materialet e trajnimit dhe shumë më tepër. Me këtë volum materiali, sigurisht që do të ketë kompromise të operacioneve të ndjeshme dhe ndoshta edhe burime njerëzore ose të infiltruarve në rrezik. Çdo operacion i krimit të organizuar ka të ngjarë të ketë kërkuar emrat e tyre përpara se zbatimi i ligjit të dijë se çfarë ka në dosje, kështu që dëmi mund të bëhet shpejt dhe të jetë i rëndë.[61]

Megjithëse ende nuk dihet se si janë marrë saktësisht skedarët BlueLeaks, dy aspekte janë të rëndësishme: a) sipas Qendrës Kombëtare të Fusionit, "Analiza paraprake e të dhënave që përmban kjo rrjedhje sugjeron se "Netsential", një kompani shërbimesh në internet e përdorur nga shumë agjenci ishte burimi i kompromentimit dhe b) përpjekjet hetimore zbuluan përdorimin e një teknike të zakonshme hakerimi për të fituar akses të gjerë në bazat e të dhënave dhe nxjerrjen e skedarëve[62]. Pas publikimit të këtij raporti, BlueLeaks mbetet në dispozicion të publikut. Në një shembull tjetër, në mars 2000, Aum Shinrikyo u zbulua se kishte software që gjurmonte 150 automjete policie. Është një pyetje e hapur nëse kjo formë e haktivizmit antiqeveritar mund të karakterizohet si një formë e veçantë e terrorizmit të nxitur nga hapësira kibernetike, pasi mund të përdoret për oficerë të veçantë të organeve ligjzbatuese apo dhe anëtarë të publikut.

[60] Greenberg, A. (2020). 'Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents', Wired (22 June). (Accessed online).

[61] Brian Krebs (2020). '"BlueLeaks" Exposes Files from Hundreds of Police Departments', KrebsOnSecurity (22 June). (Accessed online).

[62] Lee, M. (2020). 'La* Enforcement Websites Hit by BlueLeaks May Have Been Easy to Hack', The Intercept (19 August). (Accessed online).

2.4. Rast studimor - Sulmi i ransomware ndaj të dhënave mjekësore të COVID-19

Më 28 dhjetor 2020, në Antwerp, u zhvillua një sulm kibernetik që kishte në shënjestër Laboratorin e Përgjithshëm Mjekësor (AML), që analizonte rezultatet e testit Covid-19. Që herët, ishte e qartë se ky ishte sulm *ransomware*, me qëllim shantazhin për përfitime financiare. Në atë kohë, AML, një kompani private, trajtonte rreth 3,000 teste Covid-19 në ditë, ose rreth 5% të totalit kombëtar. Si e tillë, ishte një nga laboratorët më të mëdhenj privatë në vend që merrej me krizën Covid-19[63]. Një pjesë e madhe e rezultateve laboratorike, që përmbanin të dhëna për rreth një milion pacientë u bllokuan. Publikimi i të dhënave në këmbim të një shpërblimi është një formë moderne shantazhi, por asnjë e dhënë nuk arriti të përdorej. 10 ditë para sulmit të ransomware, laboratori ra pre e një sulmi tjetër kibernetik, në të cilin u gjetën malware në serverat e tij. Që nga kjo datë, e në vijim, kishte shqetësime për sulme të mëtejshme dhe akses të mundshëm të të dhënave sensitive në lidhje me Covid-19. Prandaj, sapo AML përjetoi sulmin e dytë, ajo shkëputi rrjetin e internetit. Disa javë më vonë u bë e qartë se disa laboratorë të tjerë mjekësorë (në Genk, Moeskroen, Brugge en Ardooie) kishin rënë pre e të njëjtit sulm ransomware dhe kishin pësuar pasoja të ngjashme. Që nga kjo datë, e në vijim, kishte shqetësime për sulme të mëtejshme dhe akses të mundshëm të të dhënave sensitive në lidhje me Covid-19. Prandaj, sapo AML përjetoi sulmin e dytë, ajo shkëputi rrjetin e internetit.

Disa javë më vonë u bë e qartë se disa laboratorë të tjerë mjekësorë (në Genk, Moeskroen, Brugge en Ardooie) kishin rënë pre e të njëjtit sulm ransomware dhe kishin pësuar pasoja të ngjashme.
Studimet tregojnë se sapo kompanitë sulmohen nga ransomware, mentaliteti i tyre ndryshon befas. Shumica e kompanive investojnë në parandalimin e sulmeve të reja. Çuditërisht, kjo mund të çojë në më shumë incidente[64]. Kjo është ndoshta për shkak të nivelit më të lartë të alarmit për kërcënimet e mundshme dhe përdorimit efektiv të sistemeve kundër sulmeve kibernetike. Kompanitë dhe qeveritë punësojnë më shumë specialistë të TIK, duke shpresuar se kjo do të jetë e dobishme kur të sulmohen përsëri ose kur shihen pasojat. Instalimi i sistemeve më të mira është i lidhur ngushtë me rritjen e sigurisë kibernetike dhe investimin më shumë në parandalimin e sulmeve në internet.

Impakti psikologjik

Ndërveprimi për parandalimin e sulmeve kibernetike, duke u konsideruar si profile që kërkojnë njohuri të thelluara, mund të zhvillojë një aspekt psikologjik që kërkon vëmendje më të madhe, veçanërisht në kontekstin e terrorizmit të nxitur nga hapësira kibernetike. Trajtimi i pikave të dobëta të TIK mund t›i verë stafet para niveleve të larta të stresit, për një periudhë të gjatë. Në këtë mënyrë, taktikat kundërshtare mund të ndikojnë – sipas planit ose rastësisë – në shëndetin psikologjik të stafit dhe të tjerëve.[65]

[63] (2020).'Antwerps laboratorium doelwit van ransomware', Computable (29 December).

[64] (2020). 'Ransomware-aanval verandert mentaliteit bedrijven', Computable (15 October).

[65] Chaudhury, D. (2020). 'Ransomware Is Taking a Psychological Toll on Cyber Security Experts', ITSecurity Wire, (3 November). (Accessed online); Collier, K. (2021). 'Barely Able to Keep Up: America's cyberwarriors are spread thin by attacks', NBC News (8 July). (Accessed online); Palmer, D. (2021). 'Ransomware Attacks Against Hospitals Are Having Some Very Grim Consequences', ZDNet (29 September). (Accessed online); Ranger, S. (2020). '"The Most Stressful Four Hours of My Career": Hoë it feels to be the victim of a hacking attack', ZDNet (26 June). (Accessed online).

Efekt të fortë psikologjik patën sulmet ransomware gjatë pandemisë Covid-19, duke goditur gjithçka, nga spitalet dhe shkollat tek administratat e qytetit dhe kompanitë private. Kombinimi i stresit, pafuqisë për t'u përgjigjur dhe urgjencës për të rikthyer sistemet ka kontribuar në dëshirën e shumë viktimave për të paguar shpërblimin më shpejt se në kushte jo-pandemike[66]. Deri më sot, janë bërë pak studime për këto efekte psikologjike të vazhdueshme dhe rezonuese që mund të shfaqen para, gjatë dhe pas një sulmi të madh kibernetik.

Megjithatë, mund të jetë në vetvete një taktikë për t'i bërë sulmet kibernetike më të suksesshme (për shembull, përmes lodhjes dhe stresit ndaj atyre që mbrojnë rrjetet). Profesionistët e sigurisë kibernetike, si rezultat i punës së bazuar në kibernetikë, kanë raportuar se kanë përjetuar efekte psikologjike si çrregullimi i stresit post-traumatik (PTSD).

Një grup i parë studimesh psikologjike dhe histori personale të viktimave të krimit kibernetik ofrojnë një perspektivë në natyrën e këtyre implikimeve. Analiza nga Qendra për Studime kundër Mashtrimit tregon se disa viktima të krimit kibernetik ndihen të dhunuara, sikur sulmi të ishte fizik dhe raportojnë ndikime psikologjike si zemërimi, ankthi, frika, izolimi dhe turpi[67]. Këto emocione mund të çojnë në një prishje afatgjatë të marrëdhënieve themelore të besimit, një frikë të përgjithshme nga vetë teknologjia ose në rrethana ekstreme edhe vetëvrasje.

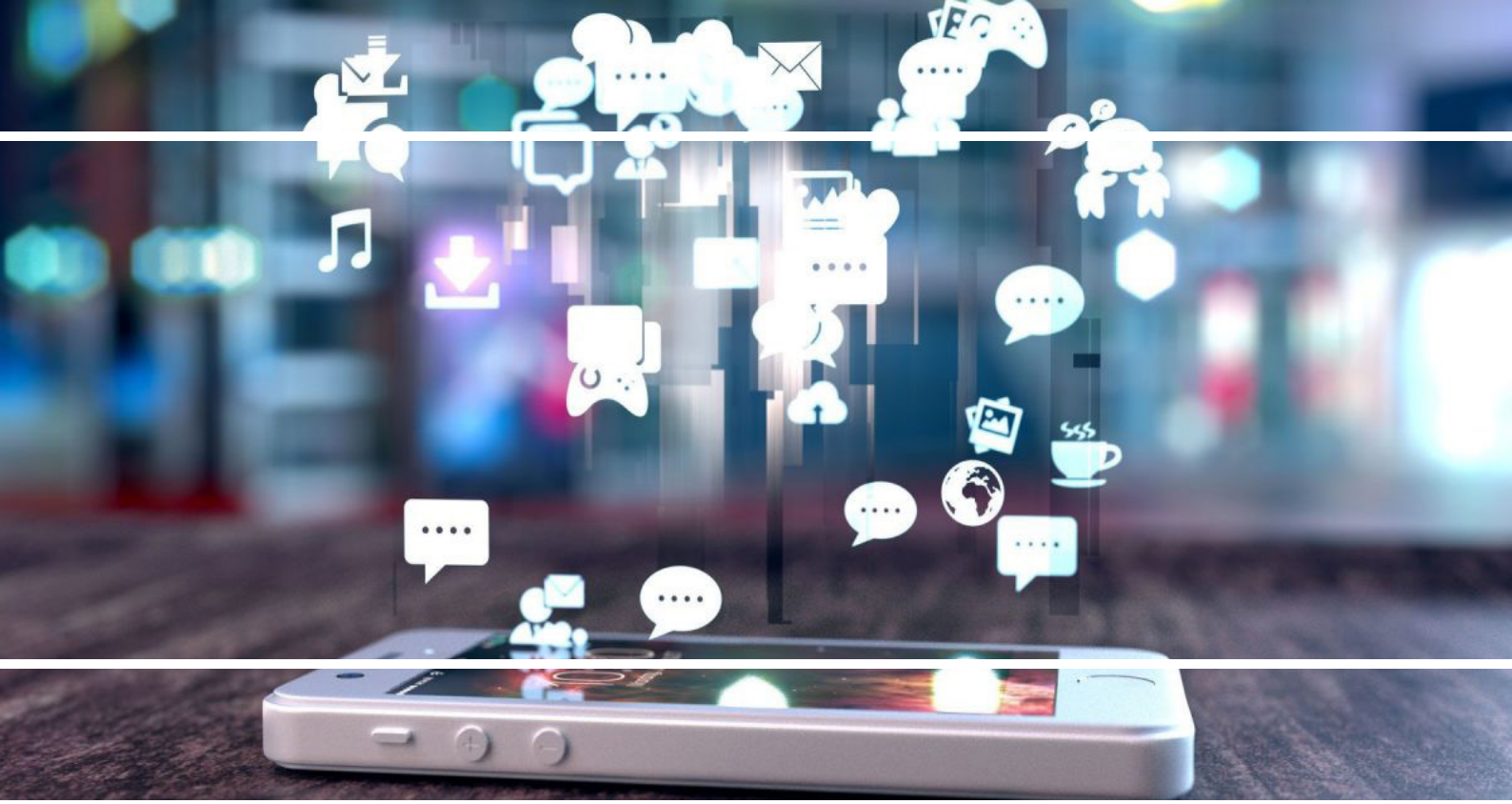
Studimet në Qendrën e Krimeve Kibernetike të Kembrixhit sugjerojnë se "në varësi të asaj se kush janë sulmuesit dhe viktimat, efektet psikologjike mund të rivalizojnë edhe ato të terrorizmit tradicional[68]".

Profesionistët e sigurisë kibernetike, që janë përballur drejtpërdrejt me përpjekje për të mbajtur rrjetin dhe të dhënat e kompanisë së tyre të sigurta, ka të ngjarë të përjetojnë efekte psikologjike. Efekte të tilla, në hakerimin e një siti finlandez lidhjesh

[66] Wilkie, C. (2021). 'Colonial Pipeline Paid $5 million Ransom One Day After Cyberattack, CEO tells Senate', CNBC (8 June). (Accessed online).

[67] Ranger. '"The Most Stressful Four Hours of My Career"

[68] Guynn, J. (2020). 'Anxiety, Depression and PTSD: The hidden epidemic of data breaches and cyber crimes', USA Today (21 February). (Accessed online).



online të terapisë Vastaamo në 2020, zbuluan informacione personale shumë të ndjeshme që shkatërruan shumë familje, çuan në vetëvrasje dhe prishën jetën e shumë të tjerëve. Të lidhura me këtë ndikim të drejtpërdrejtë psikologjik janë shqetësime të tjera mbizotëruese të kujdesit shëndetësor në komunitetin e sigurisë kibernetike që shpesh çojnë në lodhje në punë apo probleme të shëndetit mendor. Kushtet kontribuese përfshijnë mungesën e qëndrueshme të aftësive të sigurisë kibernetike (mungesa e personelit dhe qarkullimi i lartë); orë të gjata pune (stafi i mbingarkuar dhe rënia e lartë e fuqisë punëtore); kërkesa për vigjilencë të vazhdueshme (duke shkaktuar nivele të larta stresi); dhe një peisazh gjithnjë në rritje të kërcënimit kibernetik që rezulton në lodhje vigjilente[69].

Lodhja për shkak të gjendjes së përhershme të gatishmërisë kundër sulmeve është ndoshta fenomeni më interesant në këtë kontekst, sepse mund të shfaqet në kohë më të gjata të reagimit - me pasoja shkatërruese. Kjo lidhje është disi e keqpërcaktuar në literaturën akademike, por përgjithësisht pranohet se është një kombinim i desensibilizimit dhe mbingarkesës njohëse për shkak të kompleksitetit dhe sasisë së sinjalizimeve hyrëse; reagimi ndaj sinjalizimeve të veprueshme dhe humbja e kohës në ndjekjen e drejtimeve të rreme; dhe frika e vazhdueshme për të humbur një incident. Provat në lidhje me lodhjen e alarmit dërgojnë një sinjal të fortë për kompanitë dhe qeveritë që të kujdesen për stafin e sigurisë kibernetike nga perspektiva e shëndetit mendor dhe sigurisë.[70]

Përballja me rrjetet sociale

Rrjetet sociale po marrin gjithmonë e më tepër hapësirë përdorimi kryesisht tek moshat e reja por jo vetëm. Që me lindjen e rrjetit Facebook (i pari që mori një dimension global) lindi një domosdoshmëri e masës për të qenë i pranishëm në një realitet

[69] Hinkley, C. (2019). 'Preventing PTSD and Burnout for Cybersecurity Professionals', DarkReading (16 September). (Accessed online).

[70] Microsoft (2021). 'Decoding NOBELIUM: The Docuseries – Episode 4 After-Action Report'. (Accessed online).

social virtual. Ky trend u pasua nga Instagram dhe Tiktok ku numri i përdoruesve po rritet dita-ditës. Viti 2023 u mbyll me rreth 3 miliard përdorues të platformës Facebook[71], 1.35 miliard të platformës Instagram[72] dhe 800 milion të platformës Tiktok[73]. Përtej numrit të lartë të përdoruesve të rrjeteve sociale, një indikator i rëndësishëm edhe aktiviteti i përdoruesve të këtyre rrjeteve. Për vitin 2023, në platformën Facebook kemi një mesatare ditore prej 2 miliard përdoruesish aktive [74].

Ky numër kaq i lartë i llogarive në botë bën të kuptohet që shumë prej llogarive disponohen edhe nga mosha shumë të reja.

Aktiviteti i këtyre rrjeteve sociale jo gjithmonë ka një natyrë beninje. Me shqetësim vërehet një trend në rritje në aktiviteteve malinje gjatë përdorimit të rrjeteve sociale kryesisht si mashtrimi, shantazhimi dhe bullizim i përdoruesve të ndryshëm. Në veçanti:

- Mashtrimi ka si qëllim marrjen e informacioneve personale apo sensitive me anë të teknikave të "social engineering". Kjo mund të përdoret nga grupe kriminale për të përvetësuar informacione personale të cilat mund të cenojnë sigurinë e ambienteve të punës ku ato punojnë. Përdoruesi është parë gjithmonë si një hallkë e dobët për të cenuar një sistem kompjuterik. Sipas një studimi të IBM[75] dy sulmet që sëbashku zënë 31% të të gjitha sulmeve janë "phishing" dhe kredencialet e vjedhura. Një element i rëndësishëm që e mundëson mashtrimi është mundësia e "impersonifikimit" (imitimit) të një individi në rrjetet sociale. Kushdo mund të hapë një llogari me emrin e një personi tjetër, ta popullojë atë me disa nga fotot që lehtësisht mund të gjenden online dhe mashtrojë përdoruesit.

- Shantazhimi mundësohet nga lehtësia dhe nga shpejtësia me të cilën mund të përhapen informacione personale dhe sensitive në rrjetet sociale. Informacioni mund të ndahet nga përdorues identiteti i të cilëve nuk është i njohur (kjo sepse përdoruesit mund të përdorim pseudonime) si dhe informacioni i ndarë është vështirë të eliminohet plotësisht. Këto dy faktorë bëjnë që viktima të bijë pre e kërcënimeve pasi efekti negativ është tejet i lartë.

- Bullizmi mundësohet nga mungesa apo vështirësia e kontrollit të materialeve të publikuara, qoftë multimedial apo tekstual. Këto materiale kthehen një formë sulmi ndaj viktimave veçanërisht kur numri i pjesëmarrësve është i lartë.

Tiktok dhe shqetësimi multi-dimensional

Tiktok është një nga platformat më të reja që po merr një vëmendje të gjerë me përdorues që rriten dita-ditës. Mirëpo, kjo platformë është në qendër të kritikave si në aspektin social ashtu edhe politik për disa arsye:

1. Platforma po merr një përdorim të gjerë kryesisht tek moshat e reja. Megjithëse,

[71] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/
[72]https://www.statista.com/statistics/183585/instagram-number-of-global-users/
[73]https://www.statista.com/statistics/1327116/number-of-global-tiktok-users/
[74]https://www.statista.com/statistics/346167/facebook-global-dau/
[75]https://www.ibm.com/reports/data-breach

sipas kompanisë, mosha minimale për të pasur një llogari është mosha 13 vjeç (me përjashtim të disa vendeve që e kanë 14), vërehet një kontroll i munguar i kompanisë ndaj përdoruesve më të mitur të cilët janë aktiv në platformë qoftë duke publikuar materiale video qoftë në shkëmbimin e mesazheve me audiencën.

2. Materialet e publikuara ndahen me ndjekësit që cilët aksesojnë publikimet pa ndonjë konsensus paraprak. Ndryshe nga platforma Facebook apo Linkedin e cila u mundëson aksesin vetëm përdoruesve të cilët e kanë kërkuar në formë eksplicite këtë të drejtë (të ashtuquajturit "friends"), platforma Tiktok përdor përqasjen e "followers" (ndjekës). Kjo për të maksimizuar audiencën. Efektin i anësor që kushdo mund të aksesojë dhe komentojë materialet e ndara me ndjekësit. Platforma është në pronësi të kompanisë Kineze ByteDance e cila dyshohet se mbledh të dhëna sensitive të përdoruesve për tua vënë në dispozicion qeverisë Kineze. Për këtë arsye, disa vende të BE-së kanë përcaktuar një ndalim të pjesshëm të aplikacionit kryesisht për punonjësit që kanë lidhje me sigurinë apo edhe më gjerë duke përfshirë të gjithë administratën publike.

3. Ndikime në përgatitjen qytetare kundër terrorizmit kibernetik

Qytetet janë mjedise urbane komplekse – një gjurmë gjeografike me një masë njerëzish, industri dhe infrastrukturë që kryqëzohen në shtresa të ndërvarura të strukturave, sistemeve dhe shërbimeve. Ato shpesh përcaktohen nga shtrirja e tyre urbane (përhapja e strukturave të ndërtuara) dhe/ose shkalla e urbanizimit (*pjesa e popullsisë lokale që jeton brenda kufijve të qytetit*).[76] Përbërja e një qyteti zakonisht përfshin një përqindje relativisht të lartë të industrisë dhe dendësisë së popullsisë, autoritetet kombëtare dhe lokale, si dhe vende të profilit të lartë (si objektet qeveritare, infrastruktura kritike, pikat e nxehta turistike dhe vendet kulturore, arsimore etj). Qytetet kanë ndikim të rëndësishëm politik dhe ekonomik dhe autoriteteve u kërkohet të mbajnë dhe të kryejnë funksione jetësore shoqërore. Funksionet jetësore të shoqërisë në një qytet paraqesin shumë vektorë të sulmeve kibernetike, duke përfshirë infrastrukturën fizike dhe shërbimet software.

> “Ka ardhur koha për një model të ri sigurie që adreson të gjithë procesin në mënyrë holistike– para, gjatë dhe pas sulmit.”
>
> *Gordon Feller*
> *‘Protecting Our Cities from Cyber-Attacks’*

Tre faktorë thelbësorë shërbejnë si nxitës të cënueshmërisë e që ndikojnë në kërcënimin kibernetik në qytete:

1. *Ndërlidhja:* ndërlidhja e infrastrukturave që mjegullon ndarjen midis botës fizike dhe asaj online, u mundëson qyteteve të kontrollojnë dhe qeverisin sistemet teknologjike përmes operacioneve kibernetike në distancë, por kjo gjithashtu zgjeron në mënyrë eksponenciale peisazhin e kërcënimit kibernetik.
2. *Ndërveprimi:* Bashkëjetesa dhe ndërveprimet e shpeshta ndërmjet sistemeve dhe platformave të vjetra dhe të reja mund të krijojnë një ekosistem kibernetik të ndryshëm me dobësi sigurie të fshehura.
3. *Integrimi: Integrimi i teknologjive dixhitale përmes IoT dhe* dhe teknologjive dixhitale do të thotë që një problem në një zonë shërbimi mund të kalojë shpejt në zona të tjera dhe potencialisht të çojë në kërcënime të përhapura.[77]

[76] UN Habitat (no date) ‘*hat is a City?’ Accessed Online.
[77] Pandy, P. et al. ‘Making Smart Cities Cybersecure: ways to address distinct risks in an increasingly connected urban future’, Deloitte, pp. 4-7. (Accessed online).

Revolucioni digjital do të thotë se qytetet po bëhen gjithnjë e më të automatizuara, me një sërë kërcënimesh dhe teknologjish në zhvillim. Përgatitja e qyteteve për sulme kibernetike përfshin detyrën e mundimshme të korrigjimit të një cënueshmërie - për të gjetur një tjetër. Nga kjo rrjedh se aftësia e një qyteti për t'iu përgjigjur kërcënimeve kibernetike varet nga gatishmëria e tij[78]. Gatishmëria përfshin shumë faktorë, disa specifikë për rrethanat lokale, disa të zbatueshëm gjerësisht në shumicën e qyteteve. Në shumë aspekte, gatishmëria dhe qëndrueshmëria e qyteteve janë blloqet ndërtuese për gatishmërinë dhe qëndrueshmërinë e shteteve.

3.1. Siguria kibernetike në qytete

Termi "siguri kibernetike" kërkon aplikim të gjerë në kontekstin e qytetit. Ky term përfshin komunikimin e të dhënave, aksesin në shërbimet shoqërore dhe infrastrukturën kritike që mund të ndikohet nga një sulm kibernetik, si furnizimi me ujë dhe energji elektrike ose transporti.

Në kuptim strategjik, siguria e informacionit, është jetike dhe, një nga masat më të rëndësishme për një qytet për t'u forcuar në një kontekst të sigurisë kibernetike. Imagjinoni sikur dëmet e shkaktuara që ekspozojnë informacione të ndjeshme, vendndodhjet e figurave publike të profilit të lartë, korrespondenca e fshehtë, bazat e të dhënave të shërbimeve të ndërhyrjes së shpejtë, si dhe të dhënat e kujdesit shëndetësor dhe mbrojtjes sociale të vihen në rrezik për shkak të një sulmi kibernetik. Ekspozime të tilla mund të jenë të rëndësishme dhe të dëmshme, me implikime për autoritetet e qytetit dhe ndoshta sigurinë kombëtare. Mbrojtja e informacionit, sistemeve të të dhënave dhe shërbimeve software zakonisht trajtohet brenda çdo strukture përgjegjëse nëpërmjet ekspertëve të dedikuar të TIK (teknologjisë së informacionit); masat e sigurisë (për shembull, firewalls, filtrat e trafikut, balancimi i ngarkesës dhe ridrejtimi, si dhe infrastruktura e desktopit virtual); verifikimi dhe trajnimi i stafit; dhe marrëveshjet e vazhdimësisë së biznesit.

Thelbi i ndërhyrjes është të identifikohet se çfarë duhet mbrojtur, nga çfarë ka nevojë për mbrojtje dhe në çfarë mënyre ka nevojë për mbrojtje. Tradicionalisht, kjo përgjegjësi qëndron dhe duhet të zbatohet brenda çdo organizate, gjë që është e vështirë për t›u ndjekur dhe mbikëqyrur nga perspektiva e qytetit. Kjo vlen edhe për mbrojtjen e infrastrukturës kibernetike, duke përfshirë sistemet që janë të ndërlidhura, të tilla si rrjetet e rrjetit me fibra optike, por edhe sisteme kryesisht të ndara, siç janë kontrollet industriale për termocentralet. Në mënyrë tipike, këto lloje të infrastrukturës kritike operohen nga ofrues nga autoritetet kombëtare ose lokale ose nga ndërmarrje private.

3.2. Parandalimi dhe mbrojtja

Një mënyrë e qartë për të forcuar parandalimin dhe mbrojtjen është përmes promovimit të një qasjeje të fuqishme nga sektori publik dhe privat, duke kultivuar dhe zbatuar një kulturë parandalimi dhe sigurie dhe duke garantuar që kjo është thelbësore për strategjitë e sigurisë dhe zhvillimin e administratave të qytetit. Në këtë drejtim, qeverisja kibernetike është thelbësore për të vendosur politika dhe rregullore dhe për të ofruar një drejtim të qartë.

[78] Poon, L. (2021). 'What It will Take to Protect Cities Against Cyber Threats', Bloomberg CityLab. (Accessed online).

Disa standarde dhe korniza kyçe të sigurisë kibernetike të BE-së përfshijnë:

- Rregullorja e Përgjithshme për Mbrojtjen e të Dhënave GDPR: Megjithëse nuk është ekskluzivisht një standard i sigurisë kibernetike, Rregullorja e Përgjithshme për Mbrojtjen e të Dhënave (GDPR) përcakton kërkesat për mbrojtjen e të dhënave personale brenda BE-së. GDPR mandaton masat për të garantuar sigurinë dhe konfidencialitetin e të dhënave personale, duke përfshirë enkriptimin, anonimitetin dhe kërkesat e njoftimit për incidentin e sigurisë.
- Direktiva NIS: Direktiva e BE-së për sigurinë e rrjeteve dhe sistemeve të informacionit (Direktiva NIS) synon të përmirësojë pozicionin e sigurisë kibernetike të operatorëve të infrastrukturës kritike dhe ofruesve të shërbimeve dixhitale brenda BE-së. Ai kërkon që shtetet anëtare të miratojnë strategji kombëtare të sigurisë kibernetike, të krijojnë autoritetet kompetente dhe të vendosin kërkesa për raportimin e sigurisë dhe incidenteve për operatorët e infrastrukturës kritike. Në nivel ndërkombëtar, Direktiva e BE-së për Sigurinë e Rrjetit dhe Informacionit[79] ofron një shembull legjislativ, ku çdo shtet anëtar i BE-së ka filluar të miratojë legjislacionin kombëtar, i cili më pas përputhet me direktivën. Direktiva ka tre pjesë kryesore: aftësitë kombëtare, bashkëpunimi ndërkufitar dhe mbikëqyrja kombëtare e sektorëve kritikë. Për një qytet, kjo kërkon masa aktive dhe menaxhim për të përmbushur detyrimet që rrisin qëndrueshmërinë. Megjithatë, kjo shoqërohet me sfidën e përkthimit të ligjeve dhe politikave në nivel lokal si dhe në të gjithë komunitetet[80].
- ENISA: Agjencia e Bashkimit Evropian për Sigurinë Kibernetike (ENISA) ofron udhëzime, rekomandime dhe praktika më të mira për sigurinë kibernetike përmes publikimeve, raporteve dhe nismave të ndryshme. ENISA mbështet zhvillimin dhe zbatimin e standardeve të sigurisë kibernetike në të gjithë BE-në.
- ISO/IEC 27001: Edhe pse jo specifik për BE-në, ISO/IEC 27001 është një standard i njohur ndërkombëtarisht për sistemet e menaxhimit të sigurisë së informacionit (ISMS). Shumë organizata të BE-së miratojnë ISO/IEC 27001 për të krijuar dhe mbajtur praktika efektive të sigurisë kibernetike.
- Akti i sigurisë kibernetike: Akti i BE-së për sigurinë kibernetike ofron një kornizë për certifikimin e produkteve, shërbimeve dhe proceseve të sigurisë kibernetike brenda BE-së. Ai vendos Kornizën Evropiane të Certifikimit të Sigurisë Kibernetike (ECCF) për të promovuar besimin dhe besimin në produktet dhe shërbimet dixhitale.
- Skema e certifikimit të sigurisë kibernetike të BE-së për produktet, shërbimet dhe proceset e TIK-ut: Kjo skemë përshkruan kërkesat dhe kriteret specifike për certifikimin e produkteve, shërbimeve dhe proceseve të sigurisë kibernetike brenda BE-së. Ai synon të harmonizojë certifikimin e sigurisë kibernetike nëpër shtetet anëtare dhe të lehtësojë lëvizjen e lirë të produkteve dhe shërbimeve të certifikuara brenda tregut të BE-së.
- Kuadri Evropian për Certifikimin e Sigurisë Kibernetike (EFC2): EFC2 ofron një kornizë për zhvillimin e skemave të certifikimit të sigurisë kibernetike dhe marrëveshjeve të njohjes reciproke midis shteteve anëtare të BE-së. Ai mbështet krijimin e një tregu të vetëm evropian të certifikimit të sigurisë kibernetike.
- Rregullorja eIDAS: Rregullorja e Shërbimeve të Identifikimit, Autentifikimit dhe Mirëbesimit Elektronik (eIDAS) krijon një kornizë ligjore për identifikimin elektronik dhe shërbimet e besimit brenda BE-së. Ai përfshin dispozita për vërtetim të sigurt elektronik dhe nënshkrime dixhitale, duke kontribuar në sigurinë kibernetike dhe besimin në transaksionet digjitale.

[79] European Union Agency for Cybersecurity (2021). NIS 2 Directive. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new (Accessed online).
[80] Army Cyber Institute. 'Jack Voltaic 3.0', p. 8.

Strategjia e BE-së për sigurinë kibernetike për Epokën Dixhitale "tregon gjithashtu një investim të rëndësishëm në aftësinë e operacioneve të sigurisë kibernetike. Megjithatë, zbatimi në mënyrë të pashmangshme do të jetë i copëtuar dhe do të ofrojë mbrojtje të kufizuar në të gjithë zinxhirët e furnizimit".[81]

Duke kontekstualizuar *Acquis Communnaitaire* në të drejtën e brendshme, duhet theksuar se ndryshimet ligjore mbi sigurinë kibernetike të përgatitura nga Qeveria Shqiptare synojnë të adresojnë boshllëqet e deritanishme në procedura dhe masat e sigurisë. Për një përgjigje sa më efektive ndaj sfidave të sigurisë së rrjeteve dhe sistemeve të informacionit është e nevojshme një qasje gjithëpërfshirëse në nivel shtetëror dhe më gjerë në nivel ndërkombëtar, që do të përfshinte krijimin e kapaciteteve minimale, por njëkohësisht të larta dhe të mjaftueshme me qëllim planifikimin, shkëmbimin e informacionit, bashkëpunimin dhe detyrimet e përbashkëta të sigurisë për operatorët e infrastrukturave kritike të informacionit dhe operatorët e infrastrukturave të rëndësishme të informacionit.

Disa nga shkaqet kryesore të identifikuara mund të përmblidhen si më poshtë:

- Mungesa e parashikimeve të qarta ligjore lidhur me subjektet përgjegjëse të sigurisë kibernetike dhe detyrat përkatëse të tyre (CSIRT Kombëtar, CSIRT Sektorial, dhe CSIRT pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit).
- Mungesa e parashikimeve në kuadrin ligjor për ngritjen e një strukture që bën monitorimin e sigurisë kibernetike në nivel kombëtar.
- Mungesa e parashikimeve ligjore lidhur me trajtimin e gjendjes së situatave emergjente, krizës kibernetike si dhe strukturave përkatëse për menaxhimin e tyre (CERT).
- Mungesa e parashikimeve ligjore për sa i përket hartimit dhe monitorimit të Strategjisë Kombëtare të Sigurisë Kibernetike.
- Mungesa e dispozitave lidhur me certifikimin e sigurisë kibernetike dhe procedurat përkatëse.
- Mungesa e parashikimeve të qarta ligjore lidhur me administrimin e sigurisë kibernetike (masat e sigurisë, masat për menaxhimin e riskut, raportimin e incidenteve kibernetike).

Krahasuar me legjislacionin aktual, propozimet ligjore për sigurinë kibernetike në Shqipëri synojnë të përcaktojnë:

- parashikime të qarta ligjore lidhur me subjektet përgjegjëse të sigurisë kibernetike dhe detyrat përkatëse të tyre (autoritetin kombëtar përgjegjës për sigurinë kibernetike, CSIRT-in Kombëtar, CSIRT-et sektoriale, CSIRT-in pranë operatorëve të infrastrukturave të informacionit);
- ngritjen e një strukture që bën monitorimin e sigurisë në nivel kombëtar – Qendra Kombëtare Operacionale e Sigurisë Kibernetike (SOC);
- parashikimin në ligj të ngritjes së një strukture për trajtimin e situatave emergjente dhe gjendjes së krizës kibernetike – Ekipi i Përgjigjes ndaj Emergjencave të Sigurisë Kibernetike (CERT);
- garantimin e sigurisë kibernetike përmes rregullimit të certifikimit të sigurisë kibernetike në përputhje me skemat e certifikimit të Bashkimit Evropian si dhe procedurat e lidhura me to;
- parashikime të qarta ligjore lidhur me administrimin e sigurisë kibernetike, përfshirë forcimin e masave të sigurisë kibernetike, rritjen e mbikëqyrjes në kuadër të zbatimit të tyre, masat për menaxhimin e riskut,

[81] Hill and Creese. 'Why Cyber Resilience Must Be a Top-Level Leadership Strategy', p. 8.

raportimet e incidenteve të sigurisë kibernetike, raportimet vullnetare;
- rritjen e bashkëpunimit kombëtar dhe ndërkombëtar për forcimin e sigurisë kibernetike në vend dhe përmbushjen e detyrimeve ndërkombëtare në këtë fushë;

Neni 12 i këtij projektligji, përcakton identifikimin e infrastrukturave kritike dhe të rëndësishme të informacionit, autoritetet përkatëse për identifikimin e tyre, kriteret për identifikim, mënyrën e identifikimit, informacionin që duhet të jepet nga këto subjekte që do të identifikohen si infrastruktura të informacionit si dhe afatin e përditësimit të listës së këtyre infrastrukturave. Gjithashtu, ky nen përcakton se kjo listë mbahet konfidenciale. Ky parashikim vjen si rezultat i të dhënave sensitive që përmban kjo listë, ku përshkruhen emrat e sistemeve e të rrjeteve të infrastrukturave të informacionit. Ruajtja e konfidencialitetit është e domosdoshme për sigurinë e sistemeve të përmendura në të.
Nenet 20 dhe 21 trajtojnë përcaktimin e masave të sigurisë kibernetike, nivelet e tyre, institucionin përgjegjës për miratimin dhe auditimin e zbatimit të këtyre masave, zbatimin apriori të këtyre masave edhe nga ana e subjekteve që operojnë sipas këtij projektligji por që nuk janë ende pjesë e listës së infrastrukturave të informacionit, si dhe masat e ndërmarra nga operatorët e infrastrukturave kritike të informacionit dhe operatorët e infrastrukturave të rëndësishme të informacionit për menaxhimin e riskut.

Neni 22 parashikon masat e sigurisë kibernetike që merren në rast kërcënimi apo incidenti të sigurisë kibernetike, përkatësisht, masa paralajmëruese, kundërmasa dhe masa mbrojtëse të natyrës së përgjithshme. Por ky projektligj nuk ofron asnjë specifikë për përkthimin e këtyre masave në nivel vendor, për gatishmërinë e domosdoshme që kërkohen për strukturat të cilat operojnë brenda infrastrukturës fizike të një qyteti.

Sërish, qasja sikundër përcaktohet në objektin e këtij projektligji është rregullimi ligjor i përgjigjeve dhe strukturave qendrore dhe jo aq përgatitja qytetare për kërcënimet kibernetike e për më tej, sulmet kibernetike.
Neni 23 përcakton detyrimin e raportimit në rast të incidentit kibernetik nga ana e infrastrukturave të informacionit, afatin kohor për raportim në raste të incidenteve kibernetike, parametrat që duhet të merren parasysh për përcaktimin e rëndësisë së incidentit, raportet që duhen dorëzuar në rast të një incidenti kibernetik si dhe rastin kur të dhënat e administruara në lidhje me incidentet kibernetike vendosen në dispozicion të organizmave ndërkombëtarë në fushën e sigurisë kibernetike.
Klasifikimi i informacionit duket se "filtron" mbrojtjen specifike ndaj kësaj infrastrukture, por në fakt nuk orienton shpjegim mbi impaktin social, ekonomik, psikologjik në rast sulmi kibernetik mbi këto infrastruktura fizike të cilat popullohen nga qytetarë, që ofrojnë dhe marrin shërbime të ndryshme dhe që zakonisht operojnë nën administrimin e pushtetit vendor.
Transformimi teknologjik i ofrimit të shërbimeve në fakt e ka gjetur administratën e pushtetit vendor të papërgatitur për çdo skenar përgatitje, mbrojtje dhe kundërpërgjigje që kërkon zbatimi i këtij projektligji.
Përgatitja e këtij projektligji vjen pas miratimit të Strategjisë Kombëtare për Sigurinë Kibernetike dhe të planit të veprimit 2020 – 2025[82]; në fakt, duhej të kish ndodhur e kundërta për të rritur zbatueshmërinë dhe ndjekjen hap pas hapi të përgatitjes dhe qëndrueshmërisë qytetare, plotësimit me masa për fushata ndërgjegjësimi vendore; dhe, jo vetëm plotësimin me autoritete, pa përcaktuar një vlerësim të përgjithshëm të impaktit tek qytetari.

[82] Kjo Strategji eshte miratuar me VKM Nr. 1084 datë 24.12.2020

3.3. Qeverisja dhe politikat në mbrojtje të qytetarëve

Siguria kibernetike është e ngjashme me parandalimin e zjarrit; ajo ka nevojë për një qasje sistematike si pjesë e një strategjie afatgjatë do të thotë identifikimi dhe zbutja e dobësive të sistemit; forcimi i masave mbrojtëse të sigurisë dhe rregullimeve të vazhdimësisë për operacionet e qytetit; rritja e kapacitetit dhe aftësisë së agjencive për t'iu përgjigjur dhe rimëkëmbur nga një sulm... ndërkohë që zhvillon dhe integron teknologjinë (duke përdorur komponentë të testuar, të certifikuar dhe të besuar) në qytete dhe infrastrukturë në një mënyrë inteligjente.

Shërbimet e sigurisë kanë paralajmëruar se si qytetet inteligjente janë një objektiv kryesor për sulmet kibernetike, duke theksuar nevojën për të dizenjuar dhe ndërtuar "mjedise fizike të lidhura përmes internetit". Por jo gjithmonë, sistemet dhe pajisjet e integruara në infrastrukturën e qytetit (sistemet e automatizuara, sensorët, komponentët e IoT dhe të tjera) janë "të sigurta nga dizajni dhe struktura ndërtuese". Ndaj, është prioritar zbatimi i qasjeje gjithëpërfshirëse sigurie që bën bashkë teknologjinë e informacionit dhe planifikimin urban, duke synuar modelim të zgjeruar, vlerësim dhe aftësi planifikimi për politikëbërësit dhe autoritetet e sigurisë publike – si kontribut parandalues dhe mbrojtës[83].

Shumë aspekte të jetës komunitare në qytet janë "të lidhura". Ato varen nga sistemet dixhitale që kontrollojnë semaforët, pagesat elektronike, transportin, ujësjellësit, shërbimin e urgjencës mjekësore, stadiumet, tubimet dhe eventet publike etj. Aftësia për të hyrë dhe për të përcjellë informacion gjithashtu varet kryesisht nga platformat dixhitale.

Studimet evidentojnë se "garës së qyteteve dhe shteteve në mbarë botën, për të adoptuar teknologji që automatizojnë shërbimet, i dedikohen incentiva të pakëta për mbrojtjen ndaj sulmet kibernetike". E, për pasojë, edhe përgjigjet ndaj sulmeve është e ndryshme dhe kryesisht fokusohen tek funksionaliteti i teknologjisë dhe jo tek siguria publike[84].

Një shembull për këtë problematikë është rasti kur teknologjia (një dron) është përgjegjës për të kontrolluar sistemin e sensorëve të semaforëve rrugorë dhe lehtësia me të cilën një keqbërës mund të shkaktojë kaos dhe aksidente tek qytetarët përmes hakerimit të këtij droni.

Një shembull tjetër është sulm kibernetik për manipulimin e matësve inteligjentë të energjisë eletrike ndaj qytetarëve, duke krijuar ndërprerje të energjisë elektrike, apo prishje të parametrave duke shkaktuar dëmtime të rënda të aparateve që funksionojnë me energji elektrike tek përdoruesi fundor[85].

Ky është rasti i gabimit në software në disa shtete amerikane në gusht 2003, e cila rezultoi në mungesën e energjisë elektrike për 10 milionë njerëz, incidente dytësore dhe vdekje. E njëjta gjë ndodhi në dhjetor 2015 në Ukrainë, kur 225,000 klientë u prekën nga një ndërprerje e energjisë e shkaktuar nga aktorë keqdashës që kishin

[83] National Cyber Security Centre (2021). '10 Steps to Cyber Security'. (Accessed online).
[84] Wong, S. (2015). 'Cyber Attack: How easy is it to take out a smart city?', New Scientist. (Available online).
[85] ENISA (2021). 'ENISA Threat Landscape for Supply Chain Attacks', European Union Agency for Cyber Security. (Accessed online).

depërtuar në sistemet e kontrollit industrial për të fikur 30 nënstacione. Konsiderohet se furnizimi me energji elektrike është shtylla kurrizore e të gjitha funksioneve të shoqërisë. Është thelbësore për ofrimin e shërbimeve dhe nxitës i sjelljes individuale dhe kolektive [86].

Mbrojtja efektive e veprimtarisë funksionale të qyteteve dhe garantimi i shërbimeve komunitare për qytetarët kërkon jo vetëm përgjigje por përgatitje, sistematike, progresive dhe të vazhdueshme që ndërgjegjeëson çdo qytetar për të ndihmuar në reduktimin e forcës së sulmit, apo në rastin më të mirë, në devijimin e forcës së sulmeve kibernetike.

Kështu, përmendim Nju Jorkun, qytet i cili në vitin 2021 raportoi të ishte qyteti i parë me një qendër operacionale kibernetike, të gatshme për të shkëmbyer informacione në kohë reale dhe për t'u përgatitur për kërcënimet e mundshme kibernetike.

3.4. Rast Studimor – Qendra operacioneve kibernetike e New York-ut

Më 1 Prill 2019, Zyra e Prokurorit të Qarkut të Nju Jorkut, Departamenti i Policisë së qytetit të Nju Jorkut, Komanda Kibernetike e qytetit të Nju Jorkut dhe Aleanca Globale Kibernetike përuruan Qendrën e Shërbimeve dhe Infrastrukturës Kibernetike të Nju Jorkut (NYC CCSI). NYC CCSI është një bashkëpunim i profesionistëve nga njësitë publike dhe private në të gjithë sektorët e infrastrukturës kritike, që bashkohen për të luftuar kërcënimet nga kundërshtarët, në nivel global. Në vitin 2021, New York City u bë zona e parë e madhe metropolitane që hapi një qendër operacionale kibernetike, të gatshme për të shkëmbyer informacione në kohë reale dhe për t'u përgatitur për kërcënimet e mundshme kibernetike. Ajo përbëhet nga më shumë se 280 anëtarë nga 80 organizata në 12 sektorë të ndryshëm. Misioni i NYC CCSI është të ndajë informacione për kërcënimet në kohë reale dhe të dhëna të tjera përkatëse (p.sh. tregues të kompromisit), të trajnojë dhe të vendosë vullnetarë nëse një njësi ekonomike ose sektori kërkon ndihmë të specializuar.

Anëtarët e NYC CCSI janë në komunikim të vazhdueshëm nëpërmjet një kanali tw dedikuar për të siguruar që informacioni i vlefshëm po ndahet nëpër sektorë. NYC CCSI ka mbajtur disa seanca trajnimi kibernetik, ku anëtarë nga të gjithë sektorët marrin pjesë dhe kontribuojnë. Këto trajnime janë mbajtur në X-Force Cyber Range të IBM në Kembrixh, Massachusetts. Me këtë trajnim, partnerët ndanë informacione të vlefshme për kërcënimet dhe angazhohen në një sërë stërvitjesh. Bashkëpunimi i sektorëve të ndryshëm i lejon qytetit të parandalojë sulmet e mundshme kibernetike dhe të jetë gati nëse ndodh një sulm.
Gjatë pandemisë, kjo agjenci zhvilloi një seri diskutimesh me partnerë kryesorë të agjencive të sigurisë si Agjencia e Sigurisë Kibernetike dhe Sigurisë së Infrastrukturës (CISA). NYC CCSI synon të rrisë komunikimin dhe koordinimin ndërmjet sektorëve për të mbrojtur jo vetëm qytetin e Nju Jorkut, por infrastrukturën kritike në të gjithë botën përmes partnerëve globalë që përfshijnë, si Tribunal de Paris, Agjencinë për Parandalimin e Krimit Kibernetik (Liban), Europol, Departamenti Federal i Drejtësisë në Zvicer dhe Policinë e Londrës (ScotlandYard).

[86] Pescaroli, G., Turner, S., Gould, T., Alexander, D., Wicks, R. (2017). 'Cascading Impacts and Escalations in Wide-Area Power Failures', UCL IRDR and London Resilience Special Report 2017-01, Institute for Risk and Disaster Reduction, University College London, p. 4.

Ekziston nevoja për të zhvilluar marrëveshje të integruara që shoqërohen nga një grup mjetesh për të vlerësuar më mirë dobësitë në kontekstin e kërcënimeve kibernetike dhe AI. Për më tepër, një kornizë e integruar e rrezikut kibernetik për kërcënimet aktuale dhe të ardhshme, që përfshin standardet e industrisë, kërkesat ligjore dhe administrative dhe parimet e menaxhimit do t'u siguronte qyteteve një mjet për transformim[87] në drejtim të parandalimit, mbrojtjes dhe gatishmërisë.

[87] Pandy, P. et al. 'Making Smart Cities Cybersecure', p. 9.

3.5. Përgatitja përmes qasjes multi-agjenci

Gatishmëria përqendrohet në zhvillimin e planeve, procedurave dhe aranzhimeve të shumë agjencive për t'iu përgjigjur vetë sulmit kibernetik, si dhe për të reduktuar pasojat e tij. Ajo duhet të përfshijë gjithashtu mënyra të organizuara për të testuar masat mbrojtëse dhe të konsiderojë përdorimin e iniciativave krijuese, si p.sh. hackathon-et ose aktivitete të ngjashme për të forcuar sigurinë kibernetike. Këto lloje ngjarjesh po përhapen gjerësisht sepse promovojnë ndërgjegjësimin dhe bashkëpunimin, si dhe ofrojnë një mjet për të ekspozuar dhe adresuar dobësitë.

Integrimi i një planifikimi progresiv që gjeneron aftësinë për të operuar pa sisteme të caktuara dixhitale (për shembull, dokumentimi i mënyrës se si do të ndodhin vendimmarrja dhe veprimet) është thelbësor në reduktimin e ndikimit të një sulmi kibernetik. Ka të ngjarë që disa rreziqe të jenë shumë komplekse për t'u mbrojtur plotësisht, ose mbrojtja do të ishte shumë e shtrenjtë për t'u garantuar. Në këto raste, është e rëndësishme së pari të pranohet rreziku, e më pas të garantohet një qasje proporcionale për të ndërtuar gatishmërinë e

përgjithshme për të trajtuar dhe zvogëluar pasojat. "Fokusi duhet të jetë në testimin e kapacitetit për t'iu përgjigjur emergjencave dytësore që shkaktohen nga dëmtimi i infrastrukturës kritike."[88]

Sikundër në përgjigjet dhe sistemet e mbrojtjes kundër zjarrit, përmbytjeve apo forcave madhore, edhe gatishmëria e qyteteve që kanë në administrimin e tyre infrastrukturë kritike, duhet të garantohet si pjesë e detyrimeve dhe përgjegjësive ligjore dhe institucionale të bashkive dhe prefekturave – përmes hartimit dhe zbatimit të planeve të përgjigjeve ose nderhyrjeve në rast sulmi kibernetik.

Është e nevojshme që qytetet, shërbimet, agjencitë mbrojtëse dhe qytetarët si përdorues fundorë të ushtrohen përmes skenarëve të ndryshëm për mënyrat më efikase për të rritur gatishmërinë.

Një rol të rëndësishëm këtu, mund të luajnë Këshillat vendorë të sigurisë publike, të cilët janë entitete në mbrojtje të sigurisë publike dhe në reduktimin e rreziqeve që cënojnë funksionimin e qyteteve, komuniteteve, lagjeve.

[88] Coalition of City CISCO's (2021). 'Objective: Collective Defense'. (Accessed online).

Praktikimi i përgjigjes në skenarë të ndryshëm është një nga mënyrat më efikase për të rritur gatishmërinë.

3.6. Rast studimor- ushtrimi përgatitor "Thames Tideway"

Pas valës rritëse të sulmeve globale të ransomware dhe paralajmërimeve të Qendrës Kombëtare të Sigurisë Kibernetike në Mbretërinë e Bashkuar për kërcënime për sulme ndaj infrastrukturës kritike, Thames Tideway vendosi të vlerësojë gatishmërinë e saj në rast të një ngjarjeje të tillë. Në nëntor 2019, në bashkëpunim me London Resilience Group, Tideway kreu një stërvitje për menaxhimin e krizave që synonte të testonte, provonte dhe të ofronte mundësi për të zhvilluar aftësitë mbrojtëse të sigurisë kibernetike të Tideway. Skenari i ransomware ishte një ushtrim hibrid me njoftim minimal.

Planifikimi i përpiktë siguroi që çdo rrezik shoqërues të zbutej për të minimizuar ndërprerjen e biznesit.

Një ofrues i shërbimit Tideway për monitorimin e kërcënimeve (ThreatSpike Labs) mbështeti shpërndarjen e këtij ushtrimi, duke përdorur softwerin e tij duke adresuar punonjësit dhe gjeneruar ransomware të rremë, e duke përsëritur kështu një sulm kibernetik në kohë reale. Skenari nisi me një fushatë "spear-phishing", përmes emailit. U ble një emër domaini që përputhej ngushtë me adresën e emailit të Tideway që përdorej për të dërguar alarme për shëndetin dhe sigurinë. Pasi emaili dhe dokumenti bashkëlidhur u hapën, ThreatSpike përdori një listë të përcaktuar punonjësish, për të bllokuar aksesin e stafit në rrjetin personal duke nxjerrë jashtë funksioni kompjuterët të tyre. Sa më shumë punonjës e hapnin emailin, aq më shumë u shtua paniku. Ekranet e vendosura në katin e pestë dhe të gjashtë të ndërtesës së selisë filluan të shfaqnin një mesazh ransomware që kërkonte 15 milionë £ në Bitcoin në këmbim të sistemeve Tideway.

Pas elementit fillestar spear-phishing, hedhja e ransomware fokusoi kërcënimin real me të cilin përballen organizatat. Për të përmirësuar përgjigjet organizative, sulmi i ransomware u kombinua me një "kërcënim të brendshëm", një rrezik më pak i kuptuar i lidhur ngushtë me krimin kibernetik, ku stafet mund të përdorin njohuritë e tyre për sigurinë dhe praktikat e informacionit të organizatës për të zhvilluar sulm kibernetik. Shok-u dhe konfuzioni ndërmjet stafit

ishte i qartë. Departamenti i sistemeve të informacionit u trondit nga shpejtësia e sulmit fillestar. Ekipet e menaxhimit të krizave më pas ishin në gjendje të përdornin procese të strukturuara për të kuptuar situatën, për të dakordësuar prioritetet dhe për të vendosur një drejtim strategjik.

Reflektimi mbi këtë ushtrim ishte njohuritë dhe kuptueshmëria e kufizuar për sulmin ransomware dhe ndikimin e tij në sistemet e brendshme dhe vazhdimësinë e biznesit. Ndikimi i vërtetë, kostoja financiare dhe afatet kohore të rikuperimit të një sulmi të tillë gjithashtu u keqkuptuan. Ushtrimi nxiti diskutime mbi zbulimin, mënyrën se si duhet të trajtohet kërkesa për shpërblim dhe cilat agjenci partnere të përfshihen. Autoritetet e Qeverisë Qendrore të Mbretërisë së Bashkuar dhe Njësia e Krimeve Kibernetike të Shërbimit Policor Metropolitan gjithashtu vëzhguan ushtrimin dhe dhanë komente dhe këshilla të vlefshme orientuar nga përvoja me incidente reale.

Megjithëse organizatat nuk mund të mbrohen kurrë plotësisht nga krimi kibernetik, angazhimi i Tideway për të rritur ndërgjegjësimin e stafit me ekzistencën e procedurave të fuqishme dhe të praktikuara siguron që organizata të jetë në pozicionin më të mirë për t'iu përgjigjur sulmeve kibernetike.

Ushtrimi tregoi se ndërhyrjet e mirëinformuara dhe gatishmëria organizative për incidentet e tilla redukton kohën e rikuperimit. Ndërtimi i kompetencave dhe aftësive përmes trajnimeve të certifikuara për të gjitha nivelet, ushtrimet rajonale me shumë agjenci dhe ushtrimet specifike për organizatat duhet të jenë parakusht për gatishmërinë dhe reagimin kibernetik. Forumet profesionale multi-agjenci mund të jenë gjithashtu efektive në rritjen e ndërgjegjësimit dhe shkëmbimit të informacionit, konsolidimin e ekspertizës dhe veprimeve, rritjen e burimeve, si dhe mundësimin e qasjeve bashkëpunuese ndaj analizës, planifikimit dhe trajtimit të sulmeve kibernetike.

Tabela e mëposhtme përmbledh disa konsiderata kryesore në gatishmëri dhe përgjigje. Lista, natyrisht, nuk është shteruese, por ajo propozon funksione që mund të përshtaten në nivel lokal për të shërbyer si pragje për gatishmërinë ose si "nivele të qëndrueshmërisë kibernetike". Ky nocion nënkupton një progresion të pjekurisë midis niveleve, i cili teorikisht është i saktë, por do të duhej të prezantohej, testohej dhe vlerësohej në nivel lokal.

	Përgatitja	**Përgjigja**
1	Bordi i qeverisjes kibernetike Mbledhja e një bordi mbikëqyrës strategjik për të ofruar shtysën politike dhe investimin për të nxitur një qasje të koordinuar dhe progresive në një nivel të lartë, ndërsektorial të qytetit.	Grupi koordinues strategjik Organi i lartë përgjegjës, i kryesuar nga agjencia drejtuese, e cila përcakton strategjinë për të lehtësuar bashkëpunimin dhe koordinimin ndërmjet partnerëve shumë agjenci gjatë përgjigjes.
2	Strategjitë e infrastrukturës dhe qëndrueshmërisë Prezantimi dhe/ose mirëmbajtja e një kuadri të integruar të rrezikut kibernetik që lidhet me qëndrueshmërinë e qytetit dhe strategjitë e zhvillimit të infrastrukturës për të inkorporuar sigurinë kibernetike dhe marrjen në konsideratë të varësive dixhitale për të hartuar rreziqet dhe kërcënimet përkatëse.	Planet e reagimit strategjik dhe taktik Aktivizimi dhe aplikimi i planeve të përgatitura dhe aranzhimeve të paracaktuara për të udhëhequr vendimmarrjen, shpërndarjen e burimeve dhe përkthimin e strategjisë në praktikë. Planet duhet të përvijojnë struktura efikase dhe efektive për të konsoliduar dhe shkarkuar aktivitetin dhe komunikimet e shumë agjencive, si në aspektin e reagimit kibernetik ashtu edhe të menaxhimit të pasojave.
3	Trajnim dhe ushtrime me shumë agjenci Ofrimi i një programi gjithëpërfshirës trajnimi dhe ushtrimi që përfshin si seminare ashtu edhe simulime të drejtpërdrejta. Këto duhet të përfshijnë ushtrime teknike të dizajnuara për inteligjencën, ekspertët kibernetikë dhe hetuesit për të rezistuar profesionistët e fokusuar në menaxhimin e pasojave.	Njësite e kështillimit teknik të menaxhimit të pasojave dhe kibernetike Aktivizimi i grupeve të specializuara për të menaxhuar pasojat specifike. Për shembull, ndihma humanitare dhe mbështetja psikosociale, një grup rimëkëmbjeje ose komiteti i ndikimeve ekonomike, etj.
4	Grupi i gatishmërisë kibernetike dhe largpamësisë Zhvillimi i një fokus grupi që mbledh së bashku ekspertë të sigurisë kibernetike me përfaqësues ndërsektorial, të cilët kuptojnë ndikimin e mundshëm dhe implikimet e sulmeve kibernetike. Fokusi do të ishte skanimi i horizontit, zhvillimi i skenarit dhe hartëzimi i pasojave për të informuar gatishmërinë.	Njësitë e ndërgjegjësimit të situatës E informuar nga situata në kohë reale dhe gjetjet e qelizës së bashkimit të sigurisë kibernetike, qeliza e ndërgjegjësimit për situatën fokusohet në përpilimin dhe distilimin e informacionit për të identifikuar dhe kuptuar pasojat e mundshme të një kërcënimi/sulmi kibernetik të vazhdueshëm. Kjo është me qëllim të shënjimit të problemeve dhe zgjidhjeve të mundshme duke siguruar ndërgjegjësimin e përbashkët të situatës.
5	Komiteti i rishikimit të sigurisë kibernetike Një grup drejtues me shumë agjenci që monitoron tendencat, merr në konsideratë kërcënimin kibernetik, ndan të mësuarit nga çdo incident i fundit dhe merr parasysh masat teknike të sigurisë dhe marrëveshjet me shumë agjenci që mund të zbatohen për të ndihmuar në uljen e dobësive.	Qelizë e bashkimit të sigurisë kibernetike Një grup ekspertësh të inteligjencës dhe sigurisë kibernetike që mbështesin organizatat e prekura, kryejnë një vlerësim kërcënimi dhe punojnë për të zbuluar aktorët armiqësorë nëpër platforma të shumta. Ata gjithashtu mund të ofrojnë aftësinë për të analizuar rreziqet me varësi kritike për individët, organizatat dhe shoqërinë.
6	ICT organizative dhe vazhdimësia e biznesit Supozohet të jetë pozicioni bazë për shumicën e organizatave dhe shërbimeve publike. Mbikëqyrur nga një zyrtar kryesor për informacion, kjo duhet të përfshijë qeverisjen e brendshme dhe planet e vazhdimësisë; investimi në ekipe ekspertësh, mure mbrojtëse dhe sisteme dhe softuer mjaft të fuqishëm; përdorimi i shënjimit mbrojtës dhe aksesi i kufizuar sipas rastit; dhe standarde të qëndrueshme për verifikimin dhe trajnimin e stafit.	Ekipi i reagimit të urgjencës kibernetike Një ekip specialistësh specifik për organizatën e prekur që ka kualifikimet, përvojën dhe ekspertizën për të marrë vendime teknike dhe për t'i dhënë përparësi masave reaktive, të tilla si ridrejtimi, kufizimi ose mbyllja e sistemeve ndërsa përmirëson mbrojtjen kibernetike.

4. Përfundime dhe rekomandime

Rezoluta 2341 e Këshillit të Sigurimit të OKB-së për mbrojtjen e infrastrukturës kritike kundër akteve terroriste përfshin garantimin e sigurisë kibernetike si një prioritet thelbësor pë shtetet anëtare. Në këtë drejtim, kjo Rezolutë vë në dukje rëndësinë e besueshmërisë dhe qëndrueshmërisë së infrastrukturës kritike dhe mbrojtjes së saj nga sulmet terroriste ndaj sigurisë kombëtare, rendit kushtetues dhe ekonomisë së çdo shteti anëtar. Në të vërtetë, gjatë rishikimit të Strategjisë globale të OKB-së kundër terrorizmit, shtetet anëtare shprehën "shqetësim të veçantë se sulmet terroriste në infrastrukturën kritike mund të cenojnë njëlloj funksionimin e qeverisë dhe sektorit privat dhe të shkaktojnë efekte të dëmshme përtej sektorëve të përcaktuar si pjesë e infrastrukturës kritike fizike, kibernetike dhe biologjike".

Gjatë këtij procesi rishikimi, u nënvizua "rëndësia në rritje të mbrojtjes së infrastrukturës kritike nga sulmet terroriste dhe nxitja e gatishmërisë gjithëpërfshirëse, duke përfshirë partneritetin publik-privat".[89] Ky angazhim duhet të përkthehet në axhendat rajonale dhe kombëtare si dhe të gjejë kuptim dhe zbatim në prioritetet e qyteteve, për mirëqenien dhe integritetin e çdo qytetari.

Revolucioni dixhital, ndoshta si një efekt i përshpejtuar edhe për shkak të pandemisë globale[90], i katapulton qytetet në mjedise që preken nga kërcënimet e reja. Kjo mbështetet nga mënyrat e shumëanshme në të cilat aftësitë kibernetike janë përdorur nga një sërë aktorësh armiqësorë për të shkaktuar cenime të funksionimit të shtetit në nivel qendror dhe vendor.

Siç ilustrojnë shembujt e mbledhur në këtë raport, sulmet e rëndësishme kibernetike janë rritur në mënyrë eksponenciale, ndërkohë që potenciali që pasojat të tejkalojnë sulmin dhe të përhapen në shoqëri, është bërë thelbësisht i dukshëm. Dobësitë dhe kërcënimet e identifikuara japin alarmin për këtë çështje.

> "Hapësira kibernetike mbështet pothuajse çdo aspekt të jetës sonë të përditshme, shkalla dhe përhapja e 'pasigurisë' kibernetike gjithashtu njihet tani si një shqetësim kryesor."
>
> *Strategjia e Sekretarit të Përgjithshëm të Kombeve të Bashkuara për teknologjitë e reja*

[89] United Nations (2021). 'The United Nations Global Counter- Terrorism Strategy: Seventh Review'. (Accessed online).
[90] European Union Agency for Cyber Security (2020). 'The Year in Review,' p. 8. (Accessed online).

Siguria kibernetike ka rol thelbësor në sigurinë kombëtare pasi cenimi i sigurisë së rrjeteve dhe sistemeve të informacionit në Republikën e Shqipërisë do të dëmtonte interesat kombëtare dhe funksionimin e shtetit në tërësi. Për të adresuar sfidat e qeverisjes së sigurisë kibernetike dhe për të promovuar një hapësirë kibernetike të sigurt, të qëndrueshme dhe të hapur, nevojitet që korniza ligjore dhe politikat strategjike të përshtaten për të siguruar respektim dhe zbatim sa më të mirë të normave ndërkombëtare të të drejtave të njeriut, ndërsa garantojnë luftë efektive ndaj krimit kibernetik, veprimeve keqdashëse kibernetike, sulmeve kibernetike si dhe përdorimit te internetit për qëllime terroriste dhe promovimit te ekstremizmit të dhunshëm. Problematikat e evidentuara kërkojnë një legjislacion të ri dhe të përmirësuar në përputhje me Acquis e BE-së për të mundësuar garantimin dhe forcimin e sigurisë kibernetike në vend. Ndërhyrja e qeverisë është e nevojshme pasi do t'i jepte zgjidhje problematikave të përmendura më sipër që janë identifikuar gjatë zbatimit të legjislacionit ekzistues.

Gjithashtu, rishikimi i Strategjisë Kombëtare të Sigurisë Kibernetike dhe Planit të saj të Veprimit del si domosdoshmëri jo vetëm si rezultat i ndryshimeve ligjore të propozuara nëpërmjet projektligjit të ri siç janë zgjerimi i subjekteve publike dhe private, të cilat administrojnë infrastruktura të informacionit, rrjetet e komunikimit dhe sistemet e tyre, kuadrit të ri institucional që projektligji parashikon apo efektet financiare që shoqërojnë këtë projektligj për zbatimin e tij por gjithashtu edhe si reflektim i të gjitha qasjeve strategjike që Qeveria dhe shteti Shqiptar duhet të ndërtojë si rezultat i mësimeve të nxjerra nga sulmet kibernetike që vijojnë të jenë kërcënim eminent për Shqipërinë apo dhe rrjedhjeve të vazhdueshme të informacioneve sensitive të qytetarëve të saj.

Në një aspekt tjetër jo më pak të rëndësishëm, vlen të theksohet se Shqipëria gjatë procesit të rishikimit të Strategjisë Kombëtare të Sigurisë Kibernetike duhet të ketë parasysh dhe të konsiderojë qasjen e EUCSS[91], e cila fokusohet më tepër në zhvillimin e kapaciteteve, mekanizmave dhe vazhdimin e përparimeve teknologjike për të rritur standardin e sigurisë. Kjo strategji synon krijimin e një shoqërie të papenetrueshme nga sulmet kibernetike. Ndërkohë që Strategjia Kibernetike 2020-2025 e Shqipërisë mbetet ende në një fazë formuese në politikën e sigurisë kibernetike, duke vendosur si priorite kryesore rritjen e kapaciteteve në arsim, internet më të sigurt për fëmijët dhe trajnime për sigurinë kibernetike.

Në fakt, ekzistojnë pritshmëri në lidhje me përgjegjësinë sociale/shoqërore në hapësirën kibernetike ku përfshihen masat që duhet të merren për mbrojtjen e informacioneve sensitive, infrastrukturave kritike, infrastrukturave të informacionit, rrjetet e komunikimit dhe sistemet e tyre, reduktimin e terrorizmit kibernetik dhe vendosjen e fokusit tek siguria e popullatës në tërësi pasi janë individët, marrësit/përfituesit fundorë të shërbimeve publike dhe jo-publike të cilët pësojnë dëmtime më së shumti nga çdo sulm kibernetik i kryer në sistemet e informacionit.

Kur flasim për siguri kibernetike, jemi të ndërgjegjshëm se kjo është një çështje më shumë sesa vetëm teknike apo ligjore. Çështja e sigurisë kibernetike ka krijuar një perspektivë me të gjerë që shkon drejtpërdrejt tek komuniteti dhe tejkalon mbrojtjen thjesht të organizatave, institucioneve shtetërore, infrastrukturave kritike. Padyshim që, siguria e infrastrukturave të informacionit, rrjeteve të komunikimit dhe sistemet e tyre, ndërkohë që zbatohen higjena kibernetike, është shumë e rëndësishme dhe kritike dhe që duhet marrë në konsideratë për të mirën e përbashkët. Një eskpert ligjor indian i sigurisë kibernetike, Pavan Duggal[92], ka

[91] EU Cyber Security Strategy
[92] https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

thënë se *"legjislacioni kombëtar ka përdorim të kufizuar për të mbrojtur përdoruesit e një mjeti komunikimi i cili nuk ka kufi"*.

Sulmet kibernetike të vitit të shkuar që shenjëstruan institucionet shqiptare kanë rritur nevojën përpërmirësimin e sigurisë kibernetike përmes shtimit të kapaciteteve teknike dhe ligjore të nevojshme, duke përfshirë krijimin e strukturave dhe mekanizmave të nevojshme dhe përcaktimin e procedurave dhe detyrave respektive, ndërmarrjen e nismave dhe masave të shtuara, si dhe rritjen e bashkëpunimit kombëtar dhe ndërkombëtar në fushën e sigurisë kibernetike. Në këtë kuadër shihet e nevojshme rritja e nivelit të sigurisë kibernetike në vend duke krijuar strukturat e duhura për mbrojtjen efektive ndaj sulmeve të mundshme kibernetike. Duke qenë se ka një sërë institucionesh publike shtetërore të cilat janë përgjegjëse për kontrollin dhe monitorimin e aspekteve të ndryshme të sigurisë kibernetike, pra kemi një heterogjenizim të aktorëve të përfshirë dhe monitorim të fragmentuar, nevojitet një qasje më gjithëpërfshirëse dhe e integruar për të adresuar në mënyrë efektive sfidat e qeverisjes kibernetike të vendit.
Në kontekstin institucional, Parlamenti dhe deputetët luajnë një rol të padiskutueshëm në zhvillimin e kuadrit ligjor dhe institucional të sigurisë kibernetike, si dhe në garantimin që parimet e qeverisjes së mirë aplikohen në fushën e sigurisë kibernetike.

Së bashku me përgjegjësinë për miratimin e ligjeve të reja, ata gjithashtu kanë fuqinë dhe ju është dhënë rol mbikqyrës jo vetëm për të garantuar zbatimin e legjislacionit në fuqi por edhe për të mbledhur palët e interesuara për diskutime mbi politikat publike në këtë fushë, duke siguruar modele të qeverisjes gjithëpërfshirëse, me pjesëmarrje të shumë palëve - diçka që është e domosdoshme në fushën e sigurisë kibernetike për shkak të natyrës së saj ndërsektorale.

Duke marrë ne konsideratë këto përgjegjësi, është tepër e rëndësishme që, deputetët e Komisioneve Parlamentare përgjegjëse për çështje që lidhen drejtpërdrejtë ose jo të drejtpërdrejtë me sigurinë kibernetike të bashkojë përpjekjet e tyre me komisionet e tjera përgjegjëse për telekomunikacionin, arsimin, shoqërinë e informacionit dhe të drejtat e njeriut, për të përmendur vetëm disa prej tyre, duke qenë se siguria kibernetike prek jo vetëm politikën e sigurisë, por edhe fusha të tjera politike po aq të rëndësishme. Ata duhet gjithashtu të mbahen të informuar mbi zhvillimet më të fundit sai përket çështjeve të sigurisë kibernetike, duke i pajisur ata jo vetëm me njohuri por edhe me një nivel kuptueshmërie të mjaftueshme për të trajtuar çështjet dhe debatet politike mbi sigurinë kibernetike nga një pozicion ku të gjithë deputetët janë të mirinformuar.

Kapacitetet e deritanishme nuk janë të mjaftueshme për të garantuar një nivel të lartë sigurie në rrjetet dhe sistemet e informacionit. Përgatitja e përgjigjeve ndaj sulmeve apo incidenteve kibernetike nuk mjafton në nivelin që ato paraqiten, dhe kjo çon në domosdoshmërinë e ngritjes së kapaciteteve të reja teknike dhe ligjore.

Sulmet kibernetike dhe pasojat e tyre të mundshme në një mjedis urban mbeten një çështje e rrezikshme e pastudiuar në Shqipëri. Pjesërisht, kjo gjetje mund të jetë për shkak të pyetjeve të pazgjidhura në lidhje me përkufizimet dhe një perceptimi të ulët të kërcënimit bazuar në një kuptim të terrorizmit që është formuar nga dhuna fizike. Autoritetet vendore duhet të zbatojnë një qasje gjithëpërfshirëse, të orientuar drejt veprimit për të parandaluar, mbrojtur dhe për të garantuar përgatitjen për përgjigje ndaj sulmeve kibernetike. Ndaj, në këtë mënyrë, qytetet shndërrohen në komponentë thelbësore për arritjen e gatishmërisë dhe qëndrueshmërisë në nivel lokal dhe kombëtar.

Këto dinamika priren të fshehin dobësitë me të cilat përballen tashmë sistemet vendore të përgjigjes në lidhje me sulmet kibernetike që kërcënojnë humbjen e besimit të publikut tek autoritetet, ndërprerjen e shërbimeve thelbësore, ndërhyrjen në aktivitetin social politik dhe ekonomik - dhe në shprehjen më të rëndë - shkatërrimin ose humbjet fizike.
Ky raport rekomandon se një qasje gjithëpërfshirëse, e orientuar drejt veprimit duhet të bëhet prioritet për strukturat vendore dhe çdo institucion që funksionon në nivel vendor për të parandaluar, mbrojtur dhe u përgatitur për sulme kibernetike.

Pavarësisht politikave në nivel kombëtar, klasifikimit të informacionit lidhur me infrastrukturën fizike kritike, atë që preken në nivel fundor mbeten qytetarët dhe shërbimet në nivel vendor. Kjo është arsyeja pse masat e sigurisë kibernetike duhet të zbatohen, përmirësohen dhe zhvillohen në këtë nivel për të mbrojtur qytetarët dhe shërbimet.

Shqipërisë nuk i mjafton vetëm transpozimi i Aqcuis së Bashkimit Evropian (Direktivën (BE) nr.2022/2555 (NIS 2)"; për një përgjigje sa më efektive ndaj sfidave të sigurisë së rrjeteve dhe sistemeve të informacionit është e nevojshme një qasje gjithëpërfshirëse në nivel shtetëror dhe më gjerë në nivel ndërkombëtar, që do të përfshijë krijimin e kapaciteteve minimale por njëkohësisht të larta dhe të mjaftueshme me qëllim planifikimin, shkëmbimin e informacionit, bashkëpunimin dhe detyrimet e përbashkëta të sigurisë për operatorët e infrastrukturave kritike të informacionit dhe operatorët e infrastrukturave të rëndësishme të informacionit.

Rekomandime

1. Nevoja për qasje të integruar, me përfshirjen qytetare dhe aktorëve vendorë (krahas strukturave qendrore të sigurisë kombëtare) për përgatitjen dhe ndërgjegjësimin kombëtar për rrezikun nga kërcënimet apo sulmet kibernetike.
2. Rishikimi i profilit/regjistrit të kërcënimeve kibernetike/regjistrin e rrezikut dhe bërja publike e listës së kërcënimeve, përmes fushatave ndërgjegjësuese që fokusohen tek qytetarët.
3. Ndërmarrja e studimeve të thelluara dhe bërja publike e të dhënave mbi impaktin social, psikologjik, fizik dhe ekonomik që sulmet kibernetike mbartin mbi jetën dhe integritetin persona të çdo qytetari në Republikën e Shqipërisë.
4. Ndërmarrja e një analize të aftësive të reagimit kibernetik për të hartuar burimet dhe për të identifikuar boshllëqet sidomos në nivel vendor.
5. Orientimi i politikave kombëtare për përgatitjen vendore ndaj sulmeve kibernetike, duke orientuar për përgatitjen e "strategjive të ndërhyrjes në rast sulmesh kibernetike".
6. Ndërmarrja e inicitivave ndërgjegjësuese dhe angazhimi i ofruesve të internetit në diskutimin e përgjigjeve institucionale për kërcënimet e reja që vijnë përmes rrjeteve sociale.
7. Përfshirja në agjendën e Këshillave Vendore të Sigurisë Publike të diskutimit të rasteve specifike të kërcënimeve dhe sulmeve kibernetike për garantimin e rendit publik dhe mirëfunksionimit vendor të qyteteve, lagjeve dhe komuniteteve vendore.
8. Garantimi i incentivave financiare për përmirësimin e qëndrueshmërisë kibernetike ndaj çdo kërcënimi;
9. Ngritja, fuqizimi i një qendre operacionale kibernetike në nivel qyteti që mbledh së bashku ekspertët përkatës të sektorit publik, privat, shoqërisë civile dhe përfaqësues të akademisë, për të monitoruar, përgatitur dhe për t'iu përgjigjur kërcënimeve kibernetike. Kjo qendër duhet të përfshijë investime në shëndetin fizik dhe mendor të specialistëve të TIK dhe ngritje kapacitetesh.
10. Përmirësimi i marrëveshjeve të kontraktimit (përmes ndërhyrjeve shtetërore për përgatitjen e klauzolës së ruajtjes së integritetit moral dhe jetës së përdoruesve) për të nxitur investimet e operatorëve privatë për të mbrojtur grupet më të cenueshme të shoqërisë siç janë fëmijët.
11. Sinkronizimi i strategjive për të zyrtarizuar një kuadër të integruar të sigurisë kibernetike të orientuar nga veprimet. Kjo duhet të marrë në konsideratë zhvillimin e politikave dhe procedurave të shëndosha për përfshirjen e përmirësimeve të sigurisë kibernetike në ciklin jetësor të zhvillimit të infrastrukturës së strukturave vendore.

12	Planifikimi vendor dhe qendror i nevojave për investime, bazuar në pasojat e pritshme që vijnë nga harta e kërcënimeve kibernetike që mund të ndikojë në infrastrukturë dhe shërbimet kritike, dhe reduktimin e efektit "kaskadë' të përhapjes së sulmeve.
13	Intensifikim i trajnimeve dhe ushtrimet përgatitore në rast sulmesh si pjesë e një programi të koordinuar duke përdorur ushtrime "live-fire" në të gjitha nivelet (stërvitje kombëtare, rajonale dhe lokale me shumë agjenci).
14	Promovimi i parimeve bazë të "higjienës" kibernetike dhe sigurisë kibernetike dhe zbatimi i tyre si lëndë të detyrueshme mësimore në arsim. Fushatat e përgjithshme të komunikimit të sigurisë kibernetike dhe ndërgjegjësimit duhet gjithashtu të shtyhen në domeinin publik.
15	Ndarja e përvojës dhe ekspertizës dhe një qasje proaktive drejt ndërtimit të partneriteteve strategjike për të forcuar aftësitë kibernetike kundër kërcënimeve aktuale dhe atyre në zhvillim.

Table of content

1. Introduction

Studies and analysis about cyber threats and cyber attacks show that actors who organize such serious crimes that impact populations are states, organized crime' groups and other non-state actors (terrorists). The need to be prepared for and respond to terrorists seeking to take advantage of societies' increasing cyber-dependencies has been recognised by the UN Security Council through Resolution No. 2341 (2017). The Security Council calls on member states to invest in the collection and preservation of digital evidence to hold to account those responsible for terrorist attacks and to address the exploitation of information communication Technology (ICT) by terrorists[1]. The Council emphasizes how protecting critical infrastructure protection against terrorist attacks requires the convergence of multiple efforts including cyber-security[2]. The UN Office for Disarmament Affairs also convenes governmental experts to coordinate developments in the field of information and telecommunications in the context of international security [3].

> " Terrorist groups may eventually acquire the capacity to launch terrorist attacks through the Internet, thereby causing damage to critical infrastructure, industrial control systems, or Internet of Things (IoT) devices."
>
> *United Nations, "Information and communication technologies Factsheet"*

The UN highlights that, "terrorist groups may eventually acquire the capacity to launch terrorist attacks through the Internet, thereby causing damage to critical infrastructure, industrial control systems or IoT (Internet of Things) devices[4]. This program serves as an instrument to support member states in strengthening their capacities to develop and implement an effective response to this emerging threat.[5] The international community recognizes and prioritizes these issues through the Global Counter-Terrorism programme on cyber security and new technologies, which is implemented by the UN Office of Counter-Terrorism.

Regardless current knowledge and information on threats, risk or cyber attacks; the measures taken by the states (through certain policies and regulatory framework) through national security structures have not guaranteed the preparedness of all actors affected by actual threats and attacks. Mapping vulnerabilities and consequences then taking a foresight-based approach towards

[1] United Nations Security Council Counter Terrorism Committee Executive Directorate (CTED) (Unknown). 'Information and Communications Technologies Factsheet'. (Accessed online).
[2] United Nations (2017). Security Council Resolution 2341, p. 2. (Accessed online).
[3] United Nations (no date). 'Developments in the Field of Information and Telecommunications in the Context of International Security', UN Office of Disarmament Affairs. (Accessed online).
[4] United Nations Security Council Counter Terrorism Committee Executive Directorate (CTED) (Unknown). 'Information and Communications Technologies Factsheet'. (Accessed online).
[5] UNOCT (Unknown). 'Cybersecurity'. (Accessed online).

emerging threats means the implications for city preparedness can be considered. Here we talk about cities that administer objects of critical infrastructure, vital services for the population such as health services, water supply, transport, banks or local businesses[6]. This report is emphisizing the importance of addressing local and community preparedness for protecting ownself from attacks. For this reason, the analytical approach is oriented towards civic and institutional preparedness, awareness and information sharing, and extensive introduction of legislative framework regarding the potential risks of cyber terrorism.

This report is emphisizing the importance of addressing local and community preparedness for protecting ownself from attacks. For this reason, the analytical approach is oriented towards civic and institutional preparedness, awareness and information sharing, and extensive introduction of legislative framework regarding the potential risks of cyber terrorism.

This approach, in itself, is about the need for continuous citizen information and awareness, about the possible risk of cyber attacks and the preparation of local response chanels, in reducing the impact on the citizens as endusers of all goods, services and critical infrastructure. In this way, this report aims to inform and engage central and local authorities in considering preventive measures against a variety of cyber threats; as well as, efforts in reducing the risks of such attacks.

The need to increase preparedness against cyber attacks, especially those attacks with a wide impact in the real world, is the main message of this report. A sustainable and systematic strategy towards securing and protecting cyber-based systems that drive community interaction and addressing cities that manage key parts of critical infrastructure is crucial and urgent. Herein lies the delicate balance between exploiting the benefits of cyberspace and technology versus ensuring security and preparedness in the event of attacks. This need to converge cyber and physical security is an evolution in our collective journey[7].

[6] Hill, S., Creese, S. (2021). 'Why Cyber Resilience Must be a Top-Level Leadership Strategy', CAPCO Institute Journal 53: operational resilience (May), p. 82. (Accessed online).

[7] Barnard, P. (2020). 'Martyn's Law in a Security Convergent World', IFSEC Global. (Accessed online).

Understanding this level of dependency opens a window into the potential challenges presented by cyber-attacks. As technology's ability to transmit, collect, and store data matures, it will create additional attack vectors for hostile actors, including terrorists, to exploit. [8] Security studies point to the fact that "our societies rest upon a digital foundation as critical as our transportation, health, electricity, water and sewage systems".[9]

Primary focus

Cyberspace, and increasingly AI, have become the foundation of everyday technologies. Cyberspace can be defined as "a complex environment resulting from the interaction of people, software and services on the Internet by means of technological devices and networks connected to it, which does not exist in any physical form"[10]. This intangible, fluid space becomes increasingly challenging as more people, devices, systems and processes connect and interact. This fluid, intangible space becomes increasingly challenging as users, devices, systems and processes increasingly connect and interact with each other. Therefore, the use of cyberspace, artificial intelligence (AI) and advanced technologies can harm societies if used for malicious purposes by hostile actors. The UN Secretary-General's Strategy for New Technologies acknowledged both the great promise and risks these new technologies bring. The Strategy emphasizes that "while cyberspace has come to underpin almost every aspect of our daily lives, the scale and pervasiveness of 'cyber insecurity' is also now recognized as a serious concern.

The European Commission report "The Landscape of Hybrid Threats: A Conceptual Model" explores different domains of hybrid threats, including cyber threats. In this report it is also emphasized that "anything of significance in the real world also takes place in cyberspace; and therefore, the cyber dimension plays an exceptional role". The report is explicit in its statement that "cyberspace provides a new delivery mechanism that can increase the speed, diffusion and power of an attack, and ensure anonymity and undetectability. The low price of entry, anonymity and asymmetries in vulnerability mean that smaller actors have more capacity to exercise power in cyberspace than in many more traditional domains of world politics." Threat actors are now prepared to devote time and finance to strategic advantages in cyberspace [11].

In a world where low-level cyber-crime has become the norm, anyone with access to computer systems or mobile devices will be aware of phishing scams, malware attacks (especially ransomware") that bombard users daily. This view, endorsed by Interpol, highlights how cyber-crime is progressing at an incredibly fast pace, with complex criminal networks operating across the world and coordinating intricate attacks that can be executed in a master of minutes.[12] As the UK's National Security Service warns, these less visible threats have the potential to affect all of us,

[8] Devasia, Anish (2021). 'IIoT Cyber Attack Vectors and Best Mitigating Practices', Control Automation (23 July).

[9] Hill, S., Creese, S. (2021). 'Why Cyber Resilience Must be a Top-Level Leadership Strategy', CAPCO Institute Journal 53: operational resilience (May), p. 82. (Accessed online).

[10] ISO (2012). 'ISO/IEC 27032:2012: Information Technology – Security Techniques – Guidelines for Cybersecurity'. (Accessed online).

[11] Giannopoulos, G., Smith, H., Theocharidou, M. (2020). 'The Landscape of Hybrid Threats: A conceptual model', European Commission, Ispra, p. 28 (Accessed online).

[12] ISO (2012). 'ISO/IEC 27032:2012: Information Technology – Security Techniques – Guidelines for Cybersecurity'. (Accessed online).

including public services – or even worse life and human dignity.Additionally, states among themselves or in their confrontation with non-state criminal groups and individuals, can develop destabilizing approaches due to offensive postures in attributing responsibility for cyber attacks.[13]

Cyber-attacks can be employed as a tactic by any hostile actor. Although states are known to have higher levels of offensive cyber-capabilities, non-state to carry out the majority of cyber-attacks, whether actors are thought for themselves or for a state that does not want to disclose its sponsorship of the attack.[14]

Through case studies, it is concluded that societies today operate in the so-called "grey" zone, where unconventional means of attack are being transformed into instruments of hybrid warfare between peace and conflict, and are being utilized by both state and non-state actors or individuals.

Today, world practice has shown that, regardless of whether the terrorist organizations take responsibility or not for carrying out cyber-attacks, forms of recruitment and terrorist propaganda are widely spread through cyberspace.

The financing of terrorist attacks through the Internet is presented in this report as a threat to cyberspace and the need for specific legal regulation for Albania.

[13]Interpol (no date). 'Cybercrime'. (Accessed online).

[14] McCallum, K. (2021). 'Director General Annual Threat Update', UK Security Service MI5. (Accessed online).

1.1. Terminology and framing

In the context of this report, the terminology adapted in the legal package on cyber security and regulatory structures and mechanisms will be accepted and cited as defined in this legal package. This report provides an attempt to frame some specific terms that are still debateable in the international discourse on cyber risks and attacks and terrorist cyber attacks.

A cyber threat can be understood as any circumstance or event with the potential to adversely impact the operational activity of institutions, assets or individuals through unauthorized access to systems for the destruction, disclosure and modification of information and/or denial of service.[15]
In this respect, the potential for terrorist cyber-attacks against critical infrastructure is of particular importance. [16]

Cyber security risk, an identifiable event with a possible negative effect on the security of networks and information systems.

A cyber-attack as "the use of cyberspace for the purpose of disrupting, disabling, destroying or maliciously controlling a computing environment/ infrastructure; or destroying the integrity of the data or stealing controlled information".[17] It could also be understood as an event or situation caused by, or causing, a failure of electronic ICT systems that threatens serious damage to human welfare, the environment, the effective delivery of critical public services or to security.[18]

Therefore, a cyber-attack, in the context of this report, specifically refers to intentional, unlawful and significant attacks that infiltrate, exploit and/or impact upon or deny critical infrastructure, essential services and city operations with real-world implications (regardless of the initiating actor).

Analysing cyberattacks from a range of actors allows for a variety of examples to be considered in the context of terrorism. The lack of clear definitions and classification for criminal offenses related to cyber-attacks in the context of terrorism introduces subjectivity in reading this report However, this gap is mitigated by the inclusion of case studies and risk-based scenarios focused on cyber terrorism.

The term **"cyber-terrorism" kibernetik"** was coined in the late 1980s to explain the phenomenon that includes both terrorism and cyberspace.[19] In the context of the attacks of the World Trade Center in 1993, the Oklahoma bombings in 1997, and the bombings of the US embassies in Kenya and Tanzania in 1998, cyberspace was seen as a potential vector to reach connected societies through the Internet. Against this backdrop, the first reference to this issue comes through a policy paper entitled" Cyberterror: Prospects and Implications" (1999) [20], which is the first comprehensive study to address the issue of cyber-terrorism.[21]
In contrast to conventional terrorist attacks, cyber-terrorism does not necessarily threaten people

[15] Computer Security Resource Centre Glossary (no date). 'Cyber threat'. (Accessed online).
[16] United Nations (2017). Security Council Resolution 2341. (Accessed online).
[17] Computer Security Resource Centre (no date). 'Cyber Attack' definition, National Institute of Standards and Technology.
[18] Lobel-Weiss, N., Gould, T. (2019). London Cyber Incident Response Framework, London Resilience, p. 5.
[19] Emery, N.E. (2005). 'The Myth of Cyberterrorism', Journal of Information Warfare, 4(1), pp. 80-89
[20] Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., Gagnon, G. (1999). 'Cyberterror: Prospects and Implications', Defense Technical Information Center, Fort Belvoir, VA.
[21] Soesanto, S. (2020). 'Cyber Terrorism: Why it exists, Why it doesn't, and Why it Will', Real Instituto Elcano

or physical structure through violence.[22] Rather, these attacks could be operations aimed at disrupting or destroying digital property. The geopolitical context at the end of the 20th century, as well as the beginning of digitalization and debates about the "information society", further catalyzed the emergence of cyber-terrorism as a concept. Shortly after the 9/11 terrorist attack against the US, a hacker group called the Dispatchers announced that it would target countries that supported terrorists. It defaced hundreds of websites and launched Distributed Denial-of-Service/DDoS attacks against countries, including the Iranian Ministry of Interior and the presidential palace in Afghanistan, to showcase the potential impact of their capabilities[23].

Three years later, another publication, *'Terrorism in the Information Age: New Frontiers'* [24] thighlighted the vulnerability of critical infrastructure to attacks and demonstrated the interest of terrorists in targeting such "sites". Recently, the concept of cyber-terrorism has been the focus of renewed interest from academia, the media, government bodies and the international community, especially in light of the recent wave of ransomware attacks targeting or affecting critical infrastructure operators, such as its hospitals in France and Ireland, or pipeline systems and meat processing plants in the US[25].

These showed how attacks on interdependent digital data, systems or operations could manifest with far-reaching real-world implications. However, one of the main controversies regarding cyber-terrorism revolves around the definition of the concept.[26]

The concept of cyber-terrorism remains difficult to classify and distinguish from other cyber- crimes. In fact, research show that cyber-terrorism is not clearly defined under international law; and even in cases where states have tried to include cyber terrorism in their domestic legislation, they have not offered differences from other terrorist tactics.[27] This remains a challenge and raises the question of whether cyber-terrorism should be a distinct criminal offense or included in a broader understanding of terrorism. In 2021, the UN General Assembly through numerous consultations, endorsed the need to advance the responsible behaviour of member states in the use of ICTs. These consultations boost the political momentum for a more collaborative and multilateral approach. In any case, the practice will require the distinction of this criminal offense practically through the tactics of its detection, investigation and punishment.

Cyberspace-enabled terrorist: this term is focused on cases where the cyberspace serves as an enabler for the commission of terrorist acts, as well as it serves to emphasize the importance of the spread of cyber-attacks to terrorist groups. The means to deliver

[22] Denning, D.E. 'A View of Cyber-terrorism Five Years Later', Internet Security: Hacking, Counterhacking, and Society. Edited by K. Himma (Sudbury, MA: Jones and Bartlett Publishers, 2007).

[23] Denning, D. (2001). 'Is Cyber-Terror Next?', Social Science Research Council. (Accessed online).

[24] Nicander, L., Ranstorp, M. (2004). 'Terrorism in the Information Age: New frontiers?', Swedish National Defence College.

[25] Boholm, M. (2021). 'Twenty-five years of Cyber Threats in the News: A study of Swedish newspaper coverage (1995-2019)', Journal of Cybersecurity, 7(1), (Accessed 15 November 2021); 'Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment', British Journal of Political Science, pp. 1-19; Soesanto, S. (2020). 'Cyber Terrorism'.

[26] Broeders, D., Cristiano, F., Weggemans, D. (2021). 'Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy', Studies in Conflict and Terrorism, 0, pp. 1-28. (Accessed 15 November 2021); Denning, D.E. (2001). 'Activism, Hacktivism, and Cyberterrorism: The internet as a tool for influencing foreign policy', Networks and Netwars: The Future of Terror, Crime, and Militancy. Edited by J. Arquilla and D. Ronfeldt (Rand Corporation); Flemming, P., Stohl, M. (2001). 'Myths and Realities of Cyberterrorism'

[27] Straub (2020). 'Beyond Kinetic Harm'.

such an attack can affect communities and cities simply because of weak cyber systems, therefore preparedness becomes a national priority for any eventuality. This report aims to raise awareness of preparedness and the need for domestic plans that prevent terrorist cyber-attacks, through cases from different contexts and systems. The rise and consequences of cyber-attacks – notably ransomware attacks – show that the risk is increased by society's dependence upon, and interdependence with cyberspace-based systems.

The Center for Strategic and International Studies (CSIS) provides some illustrations in its published list of cyberattacks that had serious consequences: in 2015, telecommunications provider TalkTalk reported a data breach that leaked approximately 157,000 customer records, a breach that was accompanied by a "virus" email and a ransom demand[28], In 2017, the "WannaCry" attack exploded across the globe and took down parts of the United Kingdom's National Health Service (NHS).

In 2021, an attack damaged and disabled a pipeline supplying half the fuel to America's east coast; another attack attempted to poison the water supply of a city in Florida by remotely increasing the amount of sodium hydroxide[29]; and Coop Sweden closed 665 stores after point-of-sale tills and self-service checkouts stopped working due to software infiltration, thus halting the sale of fond. The latter is, of course, a small part of a much larger global supply chain attack against a major service provider that further underscores the national security dimension of the cyber-threat. According to CSIS, in the month of January 2024 alone, more than 15 cyber-attacks were carried out that targeted Canadian, Swedish, Australian government agencies, defense and technology companies, or businesses with losses in millions of dollars[30]. Cyberspace serves as an enabler for terrorism. That is not to make any claims or judgments on threat, likelihood and capability, but rather to acknowledge the capacity of cyber-attacks to expand the reach of terrorist groups. These growing trends have driven the US Department of Justice to prioritize the investigation of ransomware to the level assigned to terrorist[31], This perception of ransomware attacks, even when carried out by criminal groups, indicates the gravity with which they are viewed and the impact they can have.

"The dark web", for example, offers anonymity and the ability to malicious actors to hide and can serve as a space for discussion, coordination and action between them. It can facilitate international

[28] UK Government (2016). 'National Cyber Security Strategy 2016-2021', p. 20. (Accessed online).

[29] BBC (2021). 'Hacker Tries to Poison water Supply of Florida Cty', (February 8). (Accessed online).

[30] Center for Strategic and International Studies. 'Significant Cyber Incidents'. (Accessed online).

[31] Bing, C. (2021). 'Exclusive: US to Give Ransomware Hacks Similar Priority as Terrorism', Reuters. (Accessed online).

exchanges between hostile groups, enable access to countless forms of illegal products and criminal services. ISIS is known to have hacked into Twitter accounts[32], for example, and numerous investigations and counter terrorism operations have shown the use of encryption by Al-Qaeda and ISIS-affiliated individuals, enabling them to communicate more quickly and covertly over extended distances to foster terror on a larger scale.[33]

Recruitment, radicalisation, fundraising, dissemination of propaganda and encouragement of violence or facilitation of physical attacks are all driven through online channels. In one example, 4 fake websites from a known Islamic group used crypto-currency to finance terrorist attacks.[34] This exploitative mindset is combined with mutual exchanges of cyber expertise and training; underworld platforms on the dark web that transcend borders; clandestine networks; and a micro-economy built upon crypto-currencies."

The opportunities offered by this remote and largely untraceable space embody the very principle of cyber as a tool for malicious intent. There is a sliding scale, from terrorists using ICT for operational or other purposes all the way to terrorists that may seek to exploit cyber-technologies to attack digital, virtual or physical targets. Terrorists can take advantage of cyber dependencies and emerging technologies, which tend to be poorly regulated and governed. In 2012, after a video message from Al-Qaeda that called on its followers to carry out cyber-attacks, the concern of US law enforcement structures was to answer the question "when" rather than "if" these attacks occur.[35] Between late 2016 and early 2017, ISIS launched its first successful series of DDoS attacks, coordinated through a "dark web" space and mainly targeting government infrastructure. ISIS was reported to have used a DDoS-for-hire service, showing the link between cyber-crime and cyber-enabled terrorism.[36] The "crime-as-a-service" model raises concerns about low-skilled terrorist groups, which can purchase pre-built services or algorithms for their criminal purposes. The European Cybercrime Center now offers expertise for investigations where cyber-crime and terrorism converge.[37] Since 2017, the ISIS hacking division

[32] Hymas, C. (2019). 'ISIL Terrorists Hack Ordinary People's Dormant Twitter Accounts', The Telegraph (18 November). (Accessed online).
[33] UNOCT (2021). 'Algorithms and Terrorism: The malicious use of artificial intelligence for terrorist purposes. A Joint Report by UNICRI and UNCCT', pp. 17-18. (Accessed online).
[34] Greenberg, A. (2020). 'ISIS Allegedly Ran a Covid-19 PPE Scam Site'. (Accessed online).
[35] US Department of Justice (2012). "Assistant Attorney General for National Security Lisa Monaco Speaks at the "2012 Cybercrime Conference". (Accessed online).
[36] Flashpoint (2017). 'Cyber Jihadists Dabble in DDoS: Assessing the Threat'. (Accessed online).
[37] Europol (2021). 'European Union Terrorism Situation and Trend report', p. 105. (Accessed online).

has claimed (note: challenges in assessing the credibility of the claims are another barrier in understanding the origins of cyber-attacks) responsibility for attacks disrupting online services[38] and Europol has reported further calls from terrorist groups for cyber-attacks against sensitive targets.[39]

Hacktivism. it is considered a type of cyber terrorism or hacking, especially by certain countries under the guise of attacking political phenomena. Some of the most widespread definitions that help to understand the phenomenon are the following:

- "the nonviolent use of illegal or legally ambiguous digital means in pursuit of political goals" (Samuel, 2004)
- "A combination of political protest based on computer hacking" (Jordan and Taylor, 2004)
- "A politically motivated action, online, or community campaign undertaken by a non-state actor in retaliation to express disapproval or draw attention to a political issue" (Vegh, 2003)

Hacktivism - as a politically motivated use of hacking skills, undertaken by anonymous non-governmental actors, to spread the word, draw attention to an issue and effect change. These are the key points that help distinguish hacktivism from hacking, cyber terrorism and online activism. To provide a better understanding of what political influence can be exerted by hacktivists, we must first study the motivations behind hacktivist activities.

Cyber stability, the ability of information systems to protect data from cyber attacks, as well as the ability to resume normal work within a time, which does not affect the activity of the operator of critical or important information infrastructure, in case of a cyber attack.

[38] UNOCT (2021). 'Algorithms and Terrorism', p. 27. (Accessed online).
[39] Europol (2021). 'European Union Terrorism Situation and Trend report', p. 59. (Accessed online).

2. Vulnerability and interdependence

2.1. Information critical infrastructure

> Cyber infrastructure underpins critical infrastructure such as power plants, drinking water and wastewater facilities, hospitals, telecommunications systems, oil and gas refineries, and transport networks and national highways.
>
> *Cybersecurity and Infrastructure Security Agency (US) "Infrastructure Resilience Planning Framework"*

Cyber-attacks on critical infrastructure can cause second and third-order effects that, in some cases, cause more collateral damage than the attack itself. With the reference to domesticregulatory framework, "critical information infrastructure" means the totality of networks and information systems, owned by a public or private authority, that provide services, the violation or destruction of which would have a serious impact on health, security, economic well-being of citizens and effective functioning of the economy in the Republic of Albania. To illustrate with some examples the impact and chain effects of cyber attacks, we mention the case of Albania, in March 2021, when the cyber attack aimed at paralyzing public services and completely deleting information from the state database; resulted in the publication of personal data of citizens and state officials. In May 2021, the ransomware campaign against US oil and gas company Colonial Pipeline hit the business's IT systems and thankfully not the pipeline's flow, pressure and other metrics.[40] However, since payment information, purchase orders and inventory storage were not affected, the company was forced to take several systems offline, including the main pipelines. This decision echoed in the American ecosystem and led to disruptions in distribution, panic and lack of supply at many gas stations. Societies' demand for fuel means that such destabilization could have far-reaching effects on the functioning of cities, supply chains, economies and even international markets.

Another effect was a ransomware campaign against the Düsseldorf University Hospital (Germany) in September 2020. The ransomware infected the hospital's IT system that was used to coordinate doctors, medical treatments and bed occupancy. As this data was inaccessible, the hospital had to cancel thousands of operations, drastically limit its capacity to treat patients and stop all new admissions. The effective closure of the hospital resulted in the reporting of 2 deaths (a 78-year-old woman with an aortic aneurysm, awaiting surgery; and a case of suicide in the absence of the doctor on duty). The events were investigated and the prsecutor argued

[40] Krauss, C. et al. (2021). 'Gas Pipeline Hack Leads to Panic Buying in the South-east', The New York Times (11 May). (Accessed online).

that the first death occurred due to a health condition and not the ransomware attack. The chief public prosecutor in charge of the investigation, however, pointed to the case as "a warning sign to those running critical infrastructure" that failure to adequately protect these systems "can result in fatal outcomes".[41]

Indeed, cyber-attacks on healthcare can have serious consequences, as demonstrated by the WannaCry attack that impacted the UK healthcare system.

2.2. Case study - WannaCry ransomware attack

On Friday, May 12, 2017, a global ransomware attack, known as WannaCry, affected a wide range of countries and sectors. WannaCry infected computers running certain versions of the Microsoft Windows operating system by exploiting a specific Windows vulnerability, encrypting data and demanding ransom payments in the Bitcoin crypto-currency.

Within one day, it was reported by Europol to have infected more than 250,000 computers in at least 150 countries[42], including systems within the UK health system administration. The attack affected at least 80 out of the 236 health system insurance trusts for the financial coverage of health services across England (a) either as because some computers were infected by ransomware (b) or as a result of turning off devices as a precaution.

About 603 primary care canters and other health organizations were infected, including 595 surgical interventions. The cyber-security firm Avast identified WannaCry as one of the most widespread and most damaging cyber-attacks in history. As well as being the largest cyber-attack to affect the UK's national health system to date, WannaCry's impact was recorded as far afield as Russia, Ukraine and Taiwan, Chinese universities, Spanish Telefónica and global firms such as FedEx, Nissan and Renault.[43.]

- **British National Health System Response**

The National Health System Digital's CareCERT Service notified the Department of Health at approximately 13.00, on 12 May 2017, following multiple reports from NHS trusts. The attack was defined as a major incident to the national health system (NHS) at 16.00, warranting the implementation of a national command and control structure under existing Emergency, Preparedness, Resilience and Response plans. NHS London acted as the single point of coordination for incident management with support from the Digital Service and Support Services. From 17.00, NHS regional incident coordination centers began seeking assurance from local NHS organizations that action was being taken in line with CareCERT communications. Local organizations worked to resolve and prevent infection where possible.

Later in the evening of 12 May 2017, an expert discovered a "kill switch" version that stopped the further spread of the malware. The Digital Service wrote to all trusts on 14 May 2017 not to make any payment as a reward

[41] Ralston, W, (2020). 'The Untold Story of a Cyberattack, a Hospital and a Dying Woman', Wired (Accessed online).

[42] CNBC (2017). 'Unprecedented Cyber-Attack Hits 200,000 in At Least 150 Countries, and the Threat Is Escalating'. (Accessed online).

[43] Larson, S. (2017). 'Massive cyberattack targeting 99 countries causes sweeping havoc'. CNN. (Accessed online).

for the return of the data. [44]

The NHS response to the attack was shaped in three phases:

- Protecting emergency care pathways;
- Assuring primary care was operationally stable;
- Remediation patching, wider system actions and anti-virus update application.

In accordance with existing plans for major incident response, the NHS initially focused on maintaining emergency care services. The timing of the attack, which began on a Friday, resulted in minimal disruption to primary care services, which are usually closed over the weekend.

Over the weekend, 20 of the 25 infected trusts continued to treat emergency patients.

However, five trusts had to divert patients to other emergency departments and a smaller number needed further outside help to continue treating patients. By 16 May 2017, fewer than five hospitals were still diverting patients and several other trusts were experiencing problems with key diagnostic services. The WannaCry attack disrupted NHS services across the country until 19 May 2017, when the national incident was stood down. During this period, the Department of Health and NHS England worked with NHS Digital, the National Cyber Security Centre, the National Crime Agency and others to respond to the attack and to support NHS services in providing care to patients.

➢ Impact and lessons learned

Healthcare is a complex environment with many interconnected systems. The NHS responded effectively to this major incident, with no reports of harm or loss of patient life, or of patient data being stolen. It has been estimated by NHS England that 1% of NHS activity was directly affected by the WannaCry attack during the week of the attack. Out of 236 hospital trusts across England, 80 were severely affected, where services were impacted even if the organization was not impacted by the virus

[44] National Audit Office. 'Investigation: WannaCry cyber-attack and the NHS'. (Accessed online).

(for example, if e-mail servers or offline network connections were used). Some critical medical devices were still using Microsoft Windows 7 or XP software provided by third parties; these devices were affected, including, for example, Magnetic Resonance Imaging (MRI) scanners and blood-test analysis devices. The result was that diagnostic devices were rendered unusable as the software was running on an infected device and needed to be patched or quarantined.

NHS England identified that 6,912 appointments were cancelled and around 19,000 referral appointments were affected (deleted, changed). It is not known how many medical consultations were cancelled, or how many ambulances and patients were diverted from the five emergency departments that were unable to treat some patients. NHS England says that it is impossible to calculate with certainty the financial impact of the WannaCry attack. An overall estimate is £92 million, including service and IT costs from the attack.[45]

[45] UK Government. (2018) 'Securing Cyber Resilience in Health and Care: October 2018 update'. (Accessed online).

- **Some of the key recommendations are presented below:**

The evaluation of the Chief Information Officer concluded that the attack highlighted vulnerabilities within the NHS in England.

It exposed the need to improve the whole NHS system, including discipline and accountability around cyber security at senior leadership and board level, and the importance of systems responding quickly and effectively when new security updates are released. The assessment also highlighted historical under-investments in network security and up-to-date software.

One of the key lessons was the need for clarity on leadership and accountability for any future cyber-security incidents. This was addressed through the development of a "cyber handbook" to describe the approach and actions to be taken by NHS England, NHS Improvement and NHS Digital in the event of a cyber-attack. In principle, the Department of Health would lead the system response.

The evaluation recommended the development of local organization business-continuity, cyber-response and disaster-recovery plans to include the necessary details about cyber-incidents. This included assessing the impact of the loss of services on other parts of the health and social care system.[46] The evaluation also emphasized that plans should be regularly tested across local organizations and partners, with board-level oversight. The Digital Health Service prepared a Cyber Incident

Response Exercise [47] to support local organizations in testing incident response in health and social care.

Efforts were made to digitally transform the entire NHS service, including responsibilities for providing strategic direction for, and monitoring cyber-security. Significant work was also undertaken to develop the NHS Digital CareCERT system, which has now evolved into the Respond to an NHS cyber alert system, which allows messages to be sent to health and social care organisations, provides confirmation of receipt and receives updates on progress with remediation work. It is inevitable that health and social care systems will face attacks in the future. This requires vigilance and a process of evaluating and managing these threats.

[46] NHS England (2018). 'Lessons Learned Revieë of the WannaCry Ransomware Cyber Attack'. (Accessed online).
[47] NHS Digital. Cyber Incident Response Exercise (CIRE). (Accessed online).

As the threat landscape continues to evolve and digital systems become more and more focused on delivering healthcare to the public, there have been improvements in three key areas: cyber-monitoring, threat intelligence and incident response; support and guidance for local organizations; plus, cyber-training, awareness and engagement with cyber-security best practices.

2.3. Cyber-attacks faced by Albania

Albania's approach to cyber security is divided into two periods:

1. data leaks before 2022[48];
2. data leaks and cyber-attacks after 2022.

In 2022, Albania faced approximately 1 million cyber-attacks, with a notable 80% originating from Iran.[49]

These attacks targeted Albania's critical infrastructure, leading to a significant disruption in the country, particularly as it had recently completed the transition to providing numerous public services exclusively online. The nature and objectives of the attack fell entirely within the definition of criminal offenses associated with terrorism.

A group identifying itself as HomeLandJustice demanded that the Albanian state expel members of the MEK organization, which opposes the current regime in Iran. The group claimed that the MEK had engaged in illicit actions against Iran, contending that Albania, by hosting them, not only harbored a group labelled as terrorists by Iran, but also allowed its cyberspace to be used for conducting online terrorist activities.

Following the attack, a joint investigation conducted by the FBI and Microsoft revealed that HomeLandJustice hackers had infiltrated the system 9 months before the attack.50 This finding raised concerns in terms of the vulnerability of critical and essential infrastructures within the country.

The personal data leaks shifted the government's focus to the critical need for enhanced cyber security measures. However, a retrospective examination of the Albanian government's handling of cyber-attacks and data breaches reveals a lack of novelty or change in the employed methodology. The approach has mostly been focused on "whose fault is it" rather than "measures to be taken to avoid future occurrences".

Additionally, there is a lack of analyses regarding the societal impact and direct harm inflicted on citizens. Moreover, there is a noticeable absence of on the damages incurred by information infrastructures, critical systems, or communication networks. Such analyses should usually be carried out by all stakeholders, including institutional, public, non-public, NGOs, ICT experts, academia representatives or international experts in cooperation with each other in order to formulate plans for a coordinated response to major cyber-attacks and multidimensional preparation plans incorporating concrete steps aimed at mitigating cases of cyber-attacks or leakage of confidential, sensitive or classified state information.

During the cyber-attack, Albania was in the process

[48] The data of approximately 910,000 Albanians was exposed on the patronage list; personal data and salary details for 637,138 Albanian citizens, along with private information such as car license plates and phone numbers for 650,000 Albanians. This leaked data subsequently entered the public domain.

[49] https://kohajone.com/flet-mbreti-i-sigurise-kibernetike-shqiptare-igli-tafa/

[50] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a

of transitioning to a fully electronic governance model, exclusively delivering public services online through computer information systems.[51]

On the other hand, the National Cyber Security Strategy 2020-2025 acknowledged the lack of necessary means of the Government to provide cyber intelligence for the activity of law enforcement bodies and the lack of human resources possessing the necessary skills and qualifications to address cyber security challenges. Although the intention was to "ensure cyber security at the national level through the protection of information infrastructure", the reality proved otherwise. When faced with the cyberattacks, the government, which had been highlighting the achievements of digital governance and emphasizing public accountability, responded by presenting several arguments. Among these were assertions that the unique e-Albania government portal does not store data and that even governments with stronger cybersecurity measures have experienced similar circumstances. attacks. The government maintained that it had done its best given the

A brief overview of the cyber-attacks spanning almost two years in Albania reveals that, in the majority of instances, the primary victims are the citizens. This includes persons holding public positions as well as ordinary citizens who are users of both public and non-public services.

[51] Currently, a new law on e-government has been approved. Law No. 43/2023 "On Electronic Government".

- On July 15, 2022[52], hackers caused temporary disruptions to the websites of the Office of the Prime Minister of Albania and the Parliament, as well as the unique e-Albania government portal used to access and use public services.

- In September 2022, Albanian computer systems were targeted by Iranian hackers, forcing authorities to temporarily shut down the General Information Management System - a service used for tracking individuals entering and leaving Albania. This cyberattack was directly linked to Albania's decision to cut diplomatic ties with Iran. Prime Minister Edi Rama announced through a video statement[53] sthat the country attributed a series of severe attacks on its critical digital infrastructure earlier that summer to the Islamic Republic of Iran (IRI). Consequently, the government decided to cut diplomatic ties with Tehran, citing US sanctions and NATO condemnation in response to the Iranian cyber-attack against Albania in July. During the July attack, Iranian actors had deployed ransomware on Albanian government networks, leading to data destruction and disruptions in government services.

- On 19 September 2022, just twelve days following Albania's decision to cut diplomatic ties with the Islamic Republic of Iran, HomeLand Justice released a 47-page document on their Telegram channel. The file comprised stolen data, including personal identifying information and border crossing records of Gladis Nano, the former Director General of the State Police of Albania, and his family.

- Less than a month later, on October 3, the HomeLand Justice group once again disclosed a substantial document, this time exceeding 1.7 gigabytes in size. This document revealed the identities of 300 individuals suspected of criminal offenses in Albania. The release of such extensive data strongly implies that hackers had infiltrated Albania's sophisticated police communications system named Memex[54], raising significant concerns about the efficacy of national data protection measures.

- Following these incidents, there were ongoing periodic leaks of information. On 19 October, hackers released a file concerning the Albanian intelligence director Helidon Bendo, comprising data spanning 17 years (2005-2022) sourced from the General Information Management System (TIMS). Once again, this release exposed details of entries and exits at the state border.

- On 2 November, the group escalated its actions by disclosing the identities and personal information of 600 Albanian intelligence officers, revealing details such as names, emails, and phone numbers.

[52] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[53] https:/ / cyber-order-to-the-digital-infrastructure-of-the-government-of-the-republic-of-s/
[54] https://albanianpost.com/bie-sistemi-me-i-sofistikuar-i-komunikimit-policor-homeland-justice-vijon-publikimet-e-materialeve/

- Six days later, HomeLand Justice released a video of an Albanian intelligence operation conducted in cooperation with the State Police, which included video footage of former police chief Nano.

As emphasized in the statement by the Albanian Prime Minister on 7 September, the cyber-attacks and information disclosures in early autumn were not the initial encounters with the HomeLand Justice hacker group in the country. Earlier instances involved hackers linked to this group stealing correspondences exchanged between ministries, embassies, and even emails between the Prime Minister and Albanian citizens. The group consistently disclosed these activities on Telegram. Furthermore, on 15 July, the cyber-attackers publicly declared on Twitter their intention to carry out cyber-attacks against the National Agency for the Information Society of Albania (AKSHI), a threat they subsequently carried out.

- On 25 December 2023[55], the HomeLand Justice group managed to penetrate the data of the telecommunications company 'One', the airline company 'Air Albania' and attacked the official website of the Parliament of Albania.
- On 1 February 2024[56], the Institute of Statistics faced a cyber-attack by the HomeLand Justice group that targeted its technological infrastructure and caused considerable data damage.

Based on a risk assessment regarding the above case it can be concluded that:

Albania can be considered a "hot spot" for cyber-crimes with terrorist implications: Albania is currently subject to cyber-attacks with a terrorist nature, and there is a potential risk of it becoming a base for various organizations to launch cyber-terrorist actions against other nations.

Increase of similar attacks: *This attack may serve as an example for other terrorist groups in the future, amplifying the likelihood of similar attacks occurring. This poses an increased the risk of the spread of such attacks and the use of similar harmful tactics within Albania.*

Increasing international tensions: *Such cyber-attacks have led to the disruption of international relations between countries and lead to further diplomatic and political tensions with other countries not friendly to Albania, such as the case of Russia.*

Declining public confidence in cyber security: *Such cyberattacks can cause a decline in public confidence in cybersecurity and in the government's capacity to safeguard critical infrastructure from these risks.*

[55] https://boldnews.al/2023/12/25/one-albania-nen-kthetrat-e-homeland-justice-hakerat-sulmojne-kompanine-celulare/
[56] https://cesk.gov.al/declarate/

Preparedness to respond to cyber-attacks need to be proportionate to the risk, scale and types of services provided

A ransomware campaign targeting Toronto's public transportation ICT network in October 2021 caused the internal email system to shut down. Online bookings were unavailable and the communication system with the operators was deleted.[57] Vehicle operators switched to radio to communicate with the Control Center and passengers were encouraged to make reservations by phone. The response avoided significant service disruptions and underscored the importance of planning for reliable communications links. However, the incident resulted in the probable loss of personal information of 25,000 current and former employees.[58] An attack within cyberspace-based infrastructure can have significant cascading effects. If we consider how transport (aviation, maritime and waterborne, rail and road), power stations (electric and nuclear), water and sewage treatment plants, elevator and escalator systems, traffic lights, gas or long-distance telecommunication fibers are mostly automated. As we move to driverless cars, trucks, buses and smart homes or fully automated buildings with heating, ventilation, air conditioning, lighting and plumbing systems, the attack surface will increase. As critical infrastructure becomes increasingly digital and interconnected, the need to ensure that it is future-proofed becomes more urgent.

Communications – specifically satellite communications – have become essential for communication, geospatial positioning, environmental monitoring, data linkages and defence, which raises concerns about its vulnerability to threats such as cyber-attacks".[59]

Essential services for the community

Hostile actors including terrorists can use data theft and the aggregation of data, for example, to research, plan and support real-life (physical) attacks. The following case has been identified to show that the violation of community services can create a cascading effect that brings a wide social impact. In the case of hacking 10 years of data for about 200 police officers, training centers, support structures etc., its release to the public in mid-2020 highlighted the specific risks of political hacktivism. In the aftermath of the riots and protests in many US cities over the killing of George Floyd, DDoSecrets published this 270GB dataset known as "BlueLeaks" in June 2020.[60] TThe records came from "the largest published hack of American law enforcement agencies, and it provides the detailed information of the state local and federal agencies tasked with protecting the public, including government response to Covid-19 and the "BlackLivesMatter" protests. Although DDoSecrets deleted close to 50GB of sensitive data related to crime victims,

[57] CBC (2021). 'Toronto Transit System Hit by Ransomware Attack, TTC Says No Significant Disruptions', The Canadian Press (October 29). (Accessed online); CBC (2021). 'TTC CEO Apologizes in the wake of Ransomware Attack', CBC News (November 5). (Accessed online).

[58] Warrick, J. (2017). 'Use of weaponized Drones by ISIS Spurs Terrorism Fears', Washington Post. (Accessed online).

[59] Pescaroli, G. et al (2018). 'Increasing Resilience to Cascading Events: The M.OR.D.OR. scenario', Safety Science 110(C), Elsevier, p. 134. (Accessed online).

[60] Greenberg, A. (2020). 'Hack Brief: Anonymous Stole and Leaked a Mega-trove of Police Documents', Wired (22 June). (Accessed online).

children, healthcare and retired veterans' associations, it is believed that sensitive data was missed. Included in the millions of files is the personal information of more than 700,000 US law enforcement officers, password histories, invoices, names of informants, detailed incident maps, videos and audio files, training materials and much more.

With this volume of material, there are bound to be compromises of sensitive operations and maybe even human sources or undercover police at risk.

Every organised crime operation will likely have searched for their own names before law enforcement knows what's in the files, so the damage could be done quickly and be grave.[61]

Although it is still unknown how exactly the BlueLeaks files were taken, two aspects are noteworthy: a) according to the National Fusion Center, "Preliminary analysis of the data contained in this leak suggests that "Netsential", a web services company used by multiple agencies, was the source of the compromise"; and b) investigative efforts revealed the use of common hacking technique to gain widespread access to databases and the extraction of files.[62] Upon publication of this report, BlueLeaks remains publicly available. In a further example, Aum Shinrikyo was found to have software that tracked 150 police vehicles in March 2000.

It is an open question whether this form of anti-government hacktivism can be characterised as a distinct form of cyber-enabled terrorism, since it could be used to target specific law enforcement officers and members of the public.

[61] Brian Krebs (2020). '"BlueLeaks" Exposes Files from Hundreds of Police Departments', KrebsOnSecurity (22 June). (Accessed online).

[62] Lee, M. (2020). 'Law Enforcement Websites Hit by BlueLeaks May Have Been Easy to Hack', The Intercept (19 August). (Accessed online).

2.4. Case Study – Laboratory Ransomware attack

On 28 December 2020 a cyber-attack took place that targeted the General Medical Laboratory (GML), analysing Covid-19 test results. Early on, it was clear that this was part of a ransomware attack, aimed at blackmail for financial benefit.

At that time, GML, a private enterprise, handled about 3,000 Covid-19 tests a day, or about 5% of the national total in December 2020. As such, it was one of the largest private laboratories in the country dealing with the Covid-19 crisis.[63] A large part of the laboratories files, containing patient data of around one million people, was frozen. Extracting files in return for a ransom is a modern form of extortion but no data was used in this case. Ten days before the ransomware attack, the laboratory had been the victim of another cyber-attack, in which malware was found on the servers.

From that date onwards, there was concern about further attacks and the possible accessing of sensitive data regarding Covid-19. Therefore, as soon as the AML experienced the second attack, it disconnected the network hosting its websites.

A few weeks later it became clear that several laboratories (also those in Genk, Moeskroen, Brugge en Ardooie) had become victims of the same ransomware attack and had suffered similar consequences.

Studies show that once companies are attacked by ransomware, their mentality changes abruptly. Most companies invest in preventing new attacks. Strangely enough, this can lead to even more incidents.[64] This is probably due to the higher alert level on possible threats and the effective use of anti-cyber-attack systems. Companies and governments are hiring more ICT specialists, hoping that this will prove useful when under attack again or when the consequences are seen. Installing better systems is closely connected to enhancing cyber-security and investing more in the prevention of cyber-attacks.

Psychological impact

Interaction to prevent cyber-attacks, being considered as profiles that require deep knowledge, may develop a psychological facet that warrants closer attention, particularly in the context of cyber-enabled terrorism. Addressing ICT vulnerabilities can subject staff to high levels of stress over an extended period. In this way, adversarial tactics might – by design or coincidence – affect the psychological health of staff and others.[65]

Notably, a psycholoical effect has been at play during the ransomware campaigns during the Covid-19 pandemic, hitting everything from hospitals and schools to city administrations and private companies.

The combination of stress, helplessness and urgency to get systems back up again probably contributed to many victims' willingness not only to pay the ransom but to do so more quickly

[63] (2020)..'Antwerps laboratorium doelwit van ransomware', Computable (29 December).

[64] (2020). 'Ransomware-aanval verandert mentaliteit bedrijven', Computable (15 October).

[65] Chaudhury, D. (2020). 'Ransomware Is Taking a Psychological Toll on Cyber Security Experts', ITSecurity Wire, (3 November). (Accessed online); Collier, K. (2021). 'Barely Able to Keep Up: America's cyberwarriors are spread thin by attacks', NBC News (8 July). (Accessed online); Palmer, D. (2021). 'Ransomware Attacks Against Hospitals Are Having Some Very Grim Consequences', ZDNet (29 September). (Accessed online); Ranger, S. (2020). '"The Most Stressful Four Hours of My Career": How it feels to be the victim of a hacking attack', ZDNet (26 June). (Accessed online).

than under non-pandemic conditions.[66]

To date, little academic research has been done into these persistent and resonating psychological effects that can manifest themselves before, during and after a major cyber-attack has hit its target.

However, it could itself be a tactic to make cyber-attacks more successful (for example, through fatigue and stress on those protecting the networks). Cyber-security professionals, as a result of cyber-based work, have reported experiencing psychological effects like post-traumatic stress disorder (PTSD).

A first set of psychological studies and anecdotal accounts of cyber-crime victims offer a perspective into the nature of these implications. Analysis by the Centre for Counter Fraud Studies indicates that some cyber-crime victims feel violated, as if the attack was physical, and report psychological impacts such as anger, anxiety, fear, isolation and embarrassment.[67]

These emotions can lead to a long-term breakdown in fundamental trust relationships, a general fear of technology itself or in extreme circumstances even suicide. Research at the Cambridge Cybercrime Centre suggests that "depending on who the attackers and the victims are, the psychological effects may even rival those of traditional terrorism".[68]

Cyber-security professionals who may have struggled to keep their company's network and data secure are likely to experience psychological effects. Such effects, in the hacking of a Finnish site of Vastaamo therapy in 2020 leaked highly sensitive personal information that destroyed many families, led to suicides and derailed the lives of countless others. Related to this direct psychological impact are other prevalent

[66] Wilkie, C. (2021). 'Colonial Pipeline Paid $5 million Ransom One Day After Cyberattack, CEO tells Senate', CNBC (8 June). (Accessed online).

[67] Ranger. "The Most Stressful Four Hours of My Career".

[68] Guynn, J. (2020). 'Anxiety, Depression and PTSD: The hidden epidemic of data breaches and cyber crimes', USA Today (21 February). (Accessed online).

healthcare concerns in the cyber-security community that often lead to burnout and job fatigue. Contributing conditions include the enduring cyber-security skill shortage (understaffing and high turnover); long working hours (overworked staff and high workforce attrition); demand for persistent vigilance (causing high stress levels); and an ever-growing cyber-threat landscape that results in alert fatigue.[69]

Dealing with social networks

Social networks are getting more and more usage space mainly among young people, but not only them. Since the start of the Facebook network (the first to take on a global dimension) there was a necessity of the mass to be present in a virtual social reality. This trend was followed by Instagram and Tiktok where the number of users is increasing day by day. The year 2023 ended with about 3 billion users of the Facebook platform[70], 1.35 billion of the Instagram platform[71] and 800 million of the Tiktok platform[72]. Beyond the high number of users of social networks, the activity of users of these networks is also an important indicator. For 2023, we have a daily average of 2 billion active users on the Facebook platform.[73]

This high number of accounts in the world means that many of the accounts are available even from a very young age.

The activity of these social networks does not always have a benign nature. With concern, there is an increasing trend in malicious activities during the use of social networks,

[69] Hinkley, C. (2019). 'Preventing PTSD and Burnout for Cybersecurity Professionals', DarkReading (16 September). (Accessed online).

[70] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[71] https://www.statista.com/statistics/183585/instagram-number-of-global-users/

[72] https://www.statista.com/statistics/1327116/number-of-global-tiktok-users/

[73] https://www.statista.com/statistics/346167/facebook-global-dau/

mainly fraud, blackmail and bullying of different users. Specifically:

- Fraud aims to obtain personal or sensitive information by means of "social engineering" techniques. This can be used by criminal groups to acquire personal information which can compromise the security of the workplaces where they work. The user has always been seen as a weak link to compromise a computer system. According to an IBM study, the two attacks that together account for 31% of all attacks are "phishing" and stolen credentials. An important element that enables fraud is the possibility of "impersonating" an individual on social networks. Anyone can open an account under the name of another person, populate it with some of the photos that can easily be found online and deceive users.

- Blackmail is made possible by the ease and speed with which personal and sensitive information can be spread on social networks. Information may be shared by users whose identity is not known (this is because users may use pseudonyms) and shared information is difficult to completely eliminate. These two factors cause the victim to fall prey to threats as the negative effect is extremely high.

- Bullying is made possible by the lack or difficulty of controlling published materials, whether multimedia or textual. These materials become a form of attack on the victims especially when the number of participants is high.

Tiktok and the multi-dimensional concern

Tiktok is one of the newest platforms that is getting wide attention with users increasing day by day. However, this platform is at the center of criticism both socially and politically for several reasons:

1. The platform is getting a wide use mainly among young people. Although according to the company the minimum age to have an account is 13 years old (except in some countries where it is 14), there is a lack of control by the company towards younger users who are active on the platform either by publishing video material or in exchanging messages with the audience.

2. Published materials are shared with followers who access the publications without any prior consent. Unlike the Facebook or Linkedin platform, which allows access only to users who have explicitly requested this right (the so-called "friends"), the Tiktok platform uses the "followers" approach. This is to maximize the audience. The side effect is that anyone can access and comment on materials shared with followers.

The platform is owned by the Chinese company ByteDance, which is suspected of collecting sensitive user data to make available to the Chinese government. For this reason, some EU countries have defined a partial ban on the application mainly for security-related employees or even more widely including the entire public administration.

3. Impacts on citizen preparedness against cyber terrorism

> “It’s time for a new security model that addresses the entire attack sequele – before, during and after an attack.”
>
> *Gordon Feller ‘Protecting Our Cities from Cyber-Attacks’*

Cities are complex urban environments – a geographical footprint with a mass of people, industry and infrastructure that intersect across inherently interdependent layers of structures, systems and services. They are often defined by their urban extent (the spread of built-up structures) and/or degree of urbanisation (the share of local population living within the city’s boundaries).[74] The composition of a city usually includes a relatively high proportion of industry and population density, national and local authorities, as well as high-profile sites (such as government facilities, critical infrastructure, tourism hotspots and famous venues). Cities also wield significant political and economic influence and authorities are required to maintain and deliver vital societal functions. Vital societal functions in a city present many cyber-attack vectors, including physical infrastructure and software services.

Three core factors serve as vulnerability drivers and therefore influence the cyber-threat in cities:

1. *Interconnectivity:* the interconnectivity of infrastructures that blur the divide between physical and online worlds enables cities to control and govern technological systems through remote cyber-operations, but this also exponentially expands the cyber-threat landscape.
2. *Interoperability:* The coexistence and frequent interactions between old and new systems and platforms can create a disparate cyber-ecosystem with hidden security vulnerabilities.
3. *Integration:* Integration of digital technologies through IoT means that a problem in one service area could quickly cascade into other areas and potentially lead to widespread and catastrophic failures.[75]

The digital revolution means cities are becoming increasingly automated, with a range of emerging and converging threats

[74] UN Habitat (no date) ‘What is a City?’ Accessed Online.
[75] Pandy, P. et al. ‘Making Smart Cities Cybersecure: ways to address distinct risks in an increasingly connected urban future’, Deloitte, pp. 4-7. (Accessed online).

and technologies to match. It follows that a city's ability to respond to cyber-threats is dependent on its preparedness.[76] Preparedness includes many factors, some specific to local circumstances, some broadly applicable to most cities. In many respects, the readiness and resilience of cities are the building blocks for the readiness and resilience of nations.

3.1. Cyber-security in cities

The term "cyber-security" needs a broad application in a city context. This term includes securing data communication and access to societal services, and critical infrastructure that could be affected by a cyber-attack, such as water and power supply or transport networks.
In a strategic sense, information security is vital and one of the most important measures for a city to strengthen in a cyber-security context. Imagine if the caused
damage that expose sensitive information, the locations of high-profile public figures, confidential correspondence, emergency service databases, as well as health and social care records are put at risk because of a cyber-attack. Such exposures could be significant and detrimental, with implications for city authorities and possibly national security. The protection of information, data systems and software services is usually handled within each responsible organisation through dedicated ICT (information technology) experts; security measures (for example, firewalls, traffic filters, load balancing and re-routing, as well as virtual desktop infrastructures); the vetting and training of staff; and business-continuity arrangements.

The key is to identify what needs to be protected, what it needs protection from, and in what way it needs protection. Traditionally, this responsibility sits within, and must be applied within, each organisation, which is difficult to pursue and oversee from a city perspective. This also applies to the protection of cyber-based infrastructure, including systems that are interconnected, such as fibre-optic network grids, but also largely segregated systems, such as industrial controls for power plants. Typically, these types of critical infrastructure are operated by providers from national or local authorities or by private enterprises.

3.2. Prevention and protection

An obvious way to strengthen prevention and protection is by promoting a robust approach from the public and private sectors, cultivating and implementing a culture of deterrence and security and ensuring this is central to the security and development strategies of city administrations. In this respect, cyber-governance is essential to set policy and regulation and provide a clear direction.
At an international level, the EU Network and Information Security Directive[77] offers a legislative example, whereby every EU Member State has started to adopt national legislation, which then aligns with the directive. The directive has three main parts: national capabilities, cross-border collaboration and national supervision of critical sectors. For a city, this requires active measures and management to fulfil obligations that increase resilience. This is, however, accompanied by the challenge of translating laws and policies at the local level as well as across localities[78]

[76] Poon, L. (2021). 'What It will Take to Protect Cities Against Cyber Threats', Bloomberg CityLab. (Accessed online).

[77] European Union Agency for Cybersecurity (2021). NIS 2 Directive. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new (Accessed online).

[78] Army Cyber Institute. 'Jack Voltaic 3.0', p. 8.

Some key EU cybersecurity standards and frameworks include:

- GDPR: Although not exclusively a cybersecurity standard, the General Data Protection Regulation (GDPR) sets out requirements for the protection of personal data within the EU. The GDPR mandates measures to ensure the security and confidentiality of personal data, including encryption, anonymity and security incident notification requirements.

- NIS Directive: The EU Directive on the security of network and information systems (NIS Directive) aims to improve the cybersecurity position of critical infrastructure operators and digital service providers within the EU. It requires member states to adopt national cyber security strategies, establish competent authorities and establish security and incident reporting requirements for operators of critical infrastructure.

- ENISA: The European Union Agency for Cyber Security (ENISA) provides guidelines, recommendations and best practices for cyber security through various publications, reports and initiatives. ENISA supports the development and implementation of cybersecurity standards across the EU.

- ISO/IEC 27001 : Although not specific to the EU, ISO/IEC 27001 is an internationally recognized standard for information security management systems (ISMS). Many EU organizations adopt ISO/IEC 27001 to establish and maintain effective cyber security practices.

- Cybersecurity Act: The EU Cybersecurity Act provides a framework for the certification of cybersecurity products, services and processes within the EU. It establishes the European Cyber Security Certification Framework (ECCF) to promote trust and confidence in digital products and services.

- EU cybersecurity certification scheme for ICT products, services and processes: This scheme describes the specific requirements and criteria for the certification of cybersecurity products, services and processes within the EU. It aims to harmonize cybersecurity certification across member states and facilitate the free movement of certified products and services within the EU market.

- European Framework for Cyber Security Certification (EFC2): EFC2 provides a framework for the development of cyber security certification schemes and mutual recognition agreements between EU member states. It supports the creation of a single European cybersecurity certification market.

- eIDAS Regulation: The Electronic Identification, Authentication and Trust Services Regulation (eIDAS) creates a legal framework for electronic identification and trust services within the EU. It includes provisions for secure electronic authentication and digital signatures, contributing to cyber security and trust in digital transactions.

The EU Cybersecurity Strategy for the Digital Decade also "points to a significant investment in cybersecurity operations capability. However, implementation will inevitably be patchy and offer limited protection across supply chains".[79]

Contextualizing the *Acquis Communaitaire* in domestic law, it should be noted that the legal amendments on cyber security prepared by the Albanian Government aim to address the current gaps in security procedures and measures. For a more effective response to the security challenges of networks and information systems, a comprehensive approach is necessary at the state level and more widely at the international level, which would include the creation of minimal, but at the same time high and sufficient capacities for the purpose of planning, information exchange, cooperation and joint security obligations for operators of critical information infrastructures and operators of important information infrastructures.

Some of the main causes identified can be summarized as follows:

- Lack of clear legal provisions regarding the responsible subjects of cyber security and their respective duties (National CSIRT, Sectoral CSIRT, and CSIRT near operators of critical and important information infrastructures).
- Lack of provisions in the legal framework for the establishment of a structure that monitors cyber security at the national level.
- Lack of legal provisions related to the handling of emergency situations, the cyber crisis, as well as the relevant structures for their management (CERT).
- Lack of legal provisions regarding the drafting and monitoring of the National Cyber Security Strategy.
- Lack of provisions related to cyber security certification and related procedures.
- Lack of clear legal provisions related to the administration of cyber security (security measures, measures for risk management, reporting of cyber incidents).

Compared to the current legislation, the legal proposals for cyber security in Albania aim to define:

- clear legal provisions regarding the responsible subjects of cyber security and their respective duties (the national authority responsible for cyber security, the National CSIRT, the sectoral CSIRTs, the CSIRT at the information infrastructure operators);
- the establishment of a structure that monitors security at the national level – the National Cyber Security Operational Center (SOC);
- the provision in the law of the establishment of a structure for dealing with emergency situations and the cyber crisis state – the Cyber Security Emergency Response Team (CERT);
- guaranteeing cyber security through the regulation of cyber security certification in accordance with the certification schemes of the European Union as well as related procedures;
- clear legal provisions related to cyber security administration, including the strengthening of cyber security measures, increased supervision within their implementation, risk management measures, cyber security incident reports, voluntary reports;
- increasing national and international cooperation for strengthening cyber security in the country and fulfilling international obligations in this field;

Article 12 of this draft law defines the identification of critical and important

[79] Hill and Creese. 'Why Cyber Resilience Must Be a Top-Level Leadership Strategy', p. 8.

information infrastructures, the relevant authorities for their identification, the criteria for identification, the method of identification, the information that must be provided by these entities that will be identified as information infrastructures as well as the deadline for updating the list of these infrastructures. Also, this article stipulates that this list is kept confidential. This prediction comes as a result of the sensitive data contained in this list, which describes the names of systems and networks of information infrastructures. Maintaining confidentiality is essential to the security of the systems mentioned therein.

Articles 20 and 21 deal with the definition of cyber security measures, their levels, the institution responsible for approving and auditing the implementation of these measures, the a priori implementation of these measures also by entities operating under this draft law but which are not yet part of the list of information infrastructures, as well as the measures taken by operators of critical information infrastructures and operators of important information infrastructures for risk management.

Article 22 provides for cyber security measures that are taken in the event of a cyber security threat or incident, namely, warning measures, countermeasures and protective measures of a general nature. But this draft law does not provide any specifics for the translation of these measures at the local level, for the necessary readiness that is required for the structures that operate within the physical infrastructure of a city.

Again, the approach as defined in the scope of this draft law is the legal regulation of responses and central structures and not so much citizen preparedness for cyber threats and further, cyber-attacks.

Article 23 defines the obligation of reporting in the event of a cyber incident by information infrastructures, the time limit for reporting in the event of cyber incidents, the parameters that must be taken into account for determining the importance of the incident, the reports that must be submitted in the event of a cyber incident as well as the case when the administered data related to cyber incidents are made available to international organizations in the field of cyber security.

The classification of information seems to "filter" the specific protection against this infrastructure, but in fact it does not guide towards an explanation on the social, economic, psychological impact in the event of a cyber-attack on these physical infrastructures which are populated by citizens, who offer and receive different services and which usually operate under local government administration.

The technological transformation of service delivery has in fact found the local government administration unprepared for any preparedness, protection and response scenario that the implementation of this draft law requires.

The preparation of this draft law comes after the approval of the National Cyber Security Strategy and the 2020-2025 action plan[80]; in fact, the opposite should have happened to increase the applicability and step-by-step follow-up of civic preparedness and resilience, complementing measures for local awareness campaigns; and not simply the completion with authorities without determining a general assessment of the impact on the citizen.

[80] This Strategy is approved by DCM No. 1084 dated 24.12.2020

3.3. Governance and city policies

Cyber-security is akin to fire prevention; it needs a systematic approach as part of a long-term strategy; It means identifying and mitigating system vulnerabilities; strengthening protective security measures and continuity arrangements for city operations; enhancing the capacity and capability of agencies to respond to and recover from an attack, while developing and integrating technology (using tested, certified and trusted components) into cities and infrastructure in an intelligent way.
London's City Resilience Strategy also recognises the need to develop capabilities to respond to the consequences of a cyber emergency[81], a need that will resonate with cities globally.

However, overall preparedness for accelerating cyber-threats remains a dangerous gap. Security services have warned how smart cities are a prime target for cyber-attacks, highlighting the need to ensure that we design and build these "connected physical environments" properly. Many of the systems and devices integrated into city infrastructure (automated systems, sensors, IoT components and others) are not "secure by design". Just as systems need to be secure by design there is also a recognition that future systems and processes will need to be "resilient by design". Implementing a comprehensive security-by-design approach in ICT related to urban planning, with enhanced modelling, assessment and planning capabilities for security practitioners and policymakers, would support prevention and protection. This is through the design, refurbishment and construction of systems, services and spaces that can reduce the threat. Here we may refer to publication on understanding, designing and managing inter-connected cities[82], and the 10-step guidance on how organisations can protect themselves in cyberspace[83].
Many aspects of people's lives in a city are "connected". They depend on digital systems that control sensors, traffic lights, electronic payments, transport, water supply, medical emergency service, stadiums, public protests etc. The ability to access and convey information also largely depends on digital platforms.
With cities race to adopt technologies that automate services, security researchers have highlighted how many are not doing enough to protect against cyber-attacks. Research suggests that cities vary widely in terms of how prepared they are for possible attacks, often focusing on the functionality of technology rather than security.

Many aspects of people's lives in a city are "connected". They depend on digital systems that control sensors, traffic lights, electronic payments, transport, water supply, medical emergency service, stadiums, public protests etc. The ability to access and convey information also largely depends on digital platforms.
With cities race to adopt technologies that automate services, security researchers have highlighted how many are not doing enough to protect against cyber-attacks. Research suggests

[81] Mayor of London (2020). 'London City Resilience Strategy', Greater London Authority, pp. 51-53.

[82]UK Government (2021). 'Connected Places: Cyber Security Principles', NCSC. (Accessed online).

[83]National Cyber Security Centre (2021). '10 Steps to Cyber Security'. (Accessed online).

that cities vary widely in terms of how prepared they are for possible attacks, often focusing on the functionality of technology rather than security.[84] One example is a smart traffic light system that is controlled by a drone and the easiness of perpetrators using it, thus causing grave consequences on the citizens.

Atlanta's computer networks also suffered a cyber-attack that held the city hostage for nearly a week. Reflecting on how this was overcome, the city's former Chief Information Officer noted how "the early efforts involved figuring out what needed to be retired, streamlined, patched and modernised. One of the biggest improvements was to segment the network so hackers couldn't travel from one department's system to another, and add layers of identification requirements".

In 2021, New York was reported to be the first city to introduce a real-time cyber-operations centre to share intelligence on, and prepare for, potential cyber-threats, a model that offers a benchmark for other cities.

[84] Wong, S. (2015). 'Cyber Attack: How easy is it to take out a smart city?', New Scientist. (Available on-line).

3.4. Case study - New York City cyber operations centre

On 1 April 2019, the New York County District Attorney's Office, New York City Police Department, New York City Cyber Command and Global Cyber Alliance launched the New York City Cyber Critical Services and Infrastructure (NYC CCSI) Centre. NYC CCSI is a collaboration of professionals from both public and private entities across all sectors of critical infrastructure that unite to combat threats from adversaries globally. In 2021, New York City became the first major American metropolitan area to open a real-time operational centre to protect against cyber-security threats. It is composed of more than 280 members from 80 organisations across 12 different sectors. The NYC CCSI mission is to share real-time threat information and other relevant data (e.g., indicators of compromise), train jointly and deploy volunteers should an entity or sector require specialist assistance.

To ensure that valuable information is being shared across sectors, NYC CCSI members are in constant communication via a signal channel in which real-time threat intelligence is pushed. NYC CCSI has held several in-person cyber-training sessions and table-top exercises, where members from across all sectors participate and contribute. These trainings have been held in person at IBM's X-Force Cyber Range in Cambridge, Massachusetts. Within this cyber-training partners share valuable threat intelligence and engage in a series of drills. The collaboration of the different sectors allows the city to prevent possible cyber-attacks and to be ready should an attack take place.

During the pandemic, NYC CCSI also held a series of discussions with leading security agency partners like the Cybersecurity and Infrastructure Security Agency (CISA) and Palo Alto Networks.

NYC CCSI aims to increase communication and coordination across sectors to protect not only New York City but critical infrastructure across the world through global partners that include but are not limited to Tribunal de Paris, the Liberia Cyber Crime Prevention and Mitigation Agency, Europol, Swiss Federal Department of Justice and the City of London Police.

There is a need to develop integrated arrangements that are accompanied by a set of tools to better assess vulnerabilities in the context of cyber-threats and AI. Moreover, an integrated cyber-risk framework that considers current and future threats, incorporates industry standards, legal and regulatory requirements and management principles would provide cities with a tool for transformation[85] in terms of prevention, protection and preparedness.

[85] Pandy, P. et al. 'Making Smart Cities Cybersecure', p. 9.

3.5. Multi-agency preparedness

Preparedness will naturally centre on the development of plans, procedures and multi-agency arrangements for responding to the cyber-attack itself, as well as the consequences. It should also include organised ways to test defensive measures and consider using creative initiatives, such as a hackathon or similar to develop cyber-security further.

These types of events are becoming more popular and they promote awareness and collaboration as well as providing a means to expose and address vulnerabilities.

Integrating strong continuity planning that generates the ability to operate without certain digital systems (for example, documenting how decision-making and actions will take place) is crucial in reducing the impact of a cyber-attack. It is likely that some risks are simply too complex to protect against comprehensively, or the protection would be too expensive to build.

In those cases, it is important to acknowledge and accept the risk, then focus on a proportionate approach to build overall preparedness to handle and reduce the consequences instead. "The focus should be on testing the capacity to respond to

secondary emergencies which are caused by the failure of critical infrastructure."[86] Practising response in different scenarios is one of the most efficient ways to increase preparedness.

3.6. Case study- "Thames Tideway exercise"

Following an increase in global ransomware attacks and the UK National Cyber Security Centre's warnings of hostile actors targeting infrastructure providers, Tideway decided to gauge its preparedness for such an event. In November 2019, in collaboration with London Resilience Group, Tideway conducted a crisis-management exercise aimed to test, validate and provide opportunities to develop Tideway's cyber-security defence capabilities.

The ransomware scenario was a hybrid minimal-notice exercise. Meticulous planning ensured that any associated risks were mitigated to minimise disruption to the business. A Tideway service provider for threat monitoring (ThreatSpike Labs) supported the delivery of this exercise, using its software to target individual employees and generate fake ransomware, thus replicating a real-time cyber-attack. The scenario started with a "spear-phishing" campaign, with targeted emails sent to individuals. This was delivered by procuring a domain name that closely matched the Tideway email address that was used to send health and safety alerts.

Once the email and attachment were opened, ThreatSpike used a pre-agreed employee list to deny staff access to the network by "blue-screening" their laptops. As more members of staff opened the email, confusion and panic set in. Information display screens housed on the fifth and sixth floors of the headquarters building began to display a ransomware message demanding £15 million in Bitcoin in return for releasing Tideway systems.

After the initial spear-phishing element, the ransomware injection provided a focus on the very real threat that organisations face. To improve organisational learning, the ransomware attack was combined with an "insider threat", a less understood risk closely associated with cyber-crime, where individuals belonging to an organisation can use their knowledge of the organisation's security and information practices to orchestrate or develop the cyber-attack. The shock and confusion among staff was clear. The information systems department was soon overwhelmed and just as shocked by the speed of the initial attack. Crisis-management teams were subsequently able to use structured processes to understand the situation, agree priorities and set a strategic direction.

The key learning themes identified were that the business had limited understanding of a ransomware attack and its impact on systems and business continuity. The true impact, financial cost and recovery timescales of such an attack were also misunderstood. The exercise drove discussions on disclosure, how the ransom request should be handled, and which partner agencies to involve. Colleagues from UK Central Government and the Metropolitan Police Service's Cyber Crime Unit also observed the exercise and were able to

[86] Coalition of City CISCO's (2021). 'Objective: Collective Defense'. (Accessed online).

provide valuable feedback and advice based on real incidents.

Building competence and capabilities through certified training for all levels, regional multi-agency exercises and organisation-specific exercises should be a prerequisite for those with a stake in cyber-preparedness and response. Expert-led, multi-agency forums can also be effective in increasing awareness and information sharing, consolidating expertise and actions, enhancing resourcing as well as enabling collaborative approaches towards analysis, planning and the handling of cyber-attacks.

The table below summarises some headline considerations in preparedness and response. The list is, of course, not exhaustive but it proposes functions that can be adapted locally to serve as thresholds for preparedness or as "tiers of cyber-resilience". This notion implies a progression of maturity between the tiers, which is theoretically correct but would need to be introduced, tested and evaluated locally.

	Preparedness	**Response**
1	Cyber-governance board The convening of a strategic oversight board to provide the political impetus and investment to drive a coordinated and progressive approach at a senior, cross-sector city level.	Strategic coordinating group The senior accountable body, as chaired by the lead agency, which sets the strategy to facilitate collaboration and coordination across multi-agency partners during response
2	Infrastructure and resilience strategies The introduction and/or maintenance of an integrated cyber-risk framework that links with city resilience and infrastructure development strategies to incorporate cyber-security and the consideration of digital dependencies to design out associated risks and threats.	Strategic and tactical response plans The activation and application of prepared plans and pre-determined arrangements to guide decision-making, allocate resources and translate strategy into practice. The plans should outline efficient and effective structures to consolidate and discharge multi-agency activity and communications, both in terms of cyber-response and consequence management
3	Multi-agency training and exercising The delivery of a comprehensive training and exercising programme that incorporates both table-top workshops and live simulations. These should include technical exercises designed for intelligence, cyber-experts and investigators to resilience professionals focused on consequence management.	Consequence management and cyber technical advice units The activation of specialist groups to manage specific consequences. For example, humanitarian assistance and psychosocial support, a recovery group or economic impacts committee, etc.
4	Cyber-preparedness and foresight group The development of a focus group that brings together cyber-security experts with cross-sector representatives who understand the potential impact and implications of cyber-attacks. The focus would be horizon scanning, scenario development and consequence mapping to inform preparedness.	Situational awareness unit Informed by the real-time situation and the findings of the cyber-security fusion unit, the situational awareness unit is focused on compiling and distilling information to identify and understand the potential consequences of an ongoing cyber-threat/attack. This is with a view to flagging potential problems and solutions while ensuring shared situational awareness.
5	Cyber-security review committee A multi-agency steering group that monitors trends, considers the cyber-threat, shares learning from any recent incidents and considers technical security measures and multi-agency arrangements that could be implemented to help reduce vulnerabilities.	Cyber-security fusion cell A group of intelligence and cyber-security experts who support the affected organisations, conduct a threat assessment and work to detect hostile actors across multiple platforms. They may also offer the ability to analyse risks with critical dependencies for individuals, organisations and society.
6	Organisational ICT and business continuity Assumed to be the baseline position for the majority of public organisations and services. Overseen by a Chief Information Officer, this should include internal governance and continuity plans; investment in expert teams, protective firewalls and suitably robust systems and software; the use of protective marking and restricted access as appropriate; and consistent standards for staff vetting and training	Cyber-emergency response team A specialist team specific to the affected organisation that have the qualifications, experience and expertise to make technical decisions and prioritise reactive measures, such as re-routing, limiting or shutting down systems while enhancing cyber-defences.

> Cyberspace has come to underpin almost every aspect of our daily lives, the scale and pervasiveness of cyber 'insecurity' is also now recognised as a major concern.
>
> *United Nations 'UN Secretary-General's Strategy on New Technologies'*

Resolution 2341 of the UN Security Council on the protection of critical infrastructure against terrorist acts recognised cyber-security as a core priority.232 In this respect it noted the growing importance of ensuring reliability and resilience of critical infrastructure and its protection from terrorist attacks for national security, public safety and the economy. Indeed, during the review of the UN Global Counter-Terrorism Strategy, Member States expressed "particular concern that terrorist attacks on critical infrastructure could significantly disrupt the functioning of government and the private sector alike and cause knock-on effects beyond the infrastructure sector". They underlined "the growing importance of protecting critical infrastructure from terrorist attacks and of fostering comprehensive preparedness for such attacks, including through public-private partnership".[87] This engagement translates to regional and national agendas as well as find meaning and application in the priorities of the cities, for the welfare and integrity of every citizen.

The digital revolution, arguably accelerated as a side effect of a global pandemic,[88] catapults cities into a new threat environment. This is underpinned by the multifaceted ways in which cyber-capabilities have been used by a range of hostile actors to cause disruption and damage of the state functions both at central and local level. As demonstrated by the examples in this report, significant cyber-attacks have increased exponentially, while the potential for consequences to cascade out beyond an attack itself and into society with real-world implications is evident. The vulnerabilities and threats identified sound the alarm.

Cyber security has an essential role in national security, since the violation of the security of networks and information systems in the Republic of Albania would harm the national interests and the security of the country as a whole. In order to address the challenges of cybersecurity governance and to promote a safe, resilient and open cyberspace, the legal framework and strategic policies need to be adapted to ensure the best possible respect and implementation of international

[87]United Nations (2021). 'The United Nations Global Counter- Terrorism Strategy: Seventh Review'. (Accessed online).
[88] European Union Agency for Cyber Security (2020). 'The Year in Review,' p. 8. (Accessed online).

human rights norms, while guaranteeing the effective fight against cybercrime, malicious cyber actions, cyber-attacks as well as the use of the Internet for terrorist purposes and the promotion of violent extremism. The identified problems require a new and improved legislation in accordance with the EU Acquis to enable the guarantee and strengthening of cyber security in the country. The intervention of the government is necessary as it would provide solutions to the problems mentioned above that have been identified during the implementation of the existing legislation.

Also, the revision of the National Cyber Security Strategy and its Action Plan is necessary not only as a result of the legal amendments proposed through the new draft law such as the expansion of public and private entities that manage information infrastructures, communication networks and their systems, the new institutional framework that the draft law provides or the financial effects that accompany this draft law for its implementation, but also as a reflection of all the strategic approaches that the Government and the Albanian state must build as a result of the lessons learned from cyber-attacks that continue to be an eminent threat to Albania or the continuous leaks of sensitive information of its citizens.

In another equally important aspect, it is worth noting that Albania during the revision process of the National Cyber Security Strategy should take into account and consider the EUCSS approach[89], which focuses more on developing capabilities, mechanisms and continuing technological advances to raise the standard of security. This strategy aims to create a society impenetrable to cyber-attacks. While the 2020-2025 Cyber Strategy of Albania still remains in a formative phase in cyber security policy, setting as the main priority the increase of capabilities in education, safer internet for children and cyber security training.

In fact, there is an expectation regarding social/societal responsibility in cyberspace which includes measures to be taken to protect sensitive information, critical infrastructures, information infrastructures, communication networks and their systems, reducing cyber terrorism and establishing focus on the safety of the population as a whole since it is the individuals, the end recipients/beneficiaries of public and non-public services who suffer the most damage from any cyber-attack carried out on information systems.

When we talk about cyber security, we are aware that it is more than just a technical or legal issue. The issue of cyber security has created a broader perspective that goes directly to the community and exceeds the mere protection of organizations, state institutions, critical infrastructures. Undoubtedly, the security of information infrastructures, communication networks and their systems, while implementing cyber hygiene, is very important and critical and should be considered for the common good. An Indian cyber security legal expert, Pavan Duggal[90], has stated that **"national legislation has limited use to protect users of a means of communication which has no borders".**

Last year's cyber-attacks that targeted Albanian institutions have increased the need to improve cyber security through the addition of the necessary technical and legal capabilities, including the creation of the necessary structures and mechanisms and the definition of the respective procedures and tasks, the undertaking of initiatives and measures added, as well

[89] EU Cyber Security Strategy
[90] https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

as the increase of national and international cooperation in the field of cyber security. In this context, it is considered necessary to increase the level of cyber security in the country by creating the appropriate structures for effective protection against possible cyber-attacks. Given that there are a number of state public institutions that are responsible for controlling and monitoring different aspects of cyber security resulting in a heterogeneity of actors involved and fragmented monitoring, a more comprehensive and integrated approach is needed to effectively address the country's cyber governance challenges.

In the institutional context, Parliament and MPs play an indisputable role in developing the legal and institutional framework of cyber security, as well as in ensuring that the principles of good governance are applied in the field of cyber security.

Along with the responsibility for passing new laws, they also have the power and are given an oversight role not only to ensure the implementation of existing legislation but also to convene stakeholders for public policy discussions in this area, ensuring inclusive, multi-stakeholder governance models - something that is imperative in the field of cyber security due to its cross-sectoral nature.

Taking these responsibilities into consideration, it is extremely important that the MPs of the Parliamentary Committees responsible for issues directly or indirectly related to cyber security join their efforts with other committees responsible for telecommunications, education, information society and human rights, to name just a few of them, since cyber security affects not only security policy, but also other equally important policy areas. They should also be kept informed of the latest developments in cyber security issues, equipping them not only with the knowledge but also with a level of understanding sufficient to approach the policy issues and debates on cyber security from a position where all MPs are well informed.

The current capabilities are not sufficient to guarantee a high level of security in networks and information systems. Preparing responses to cyber-attacks or incidents is not enough at the level they appear, and this leads to the necessity of building new technical and legal capabilities.

Cyber-attacks and their possible consequences in an urban environment remain a dangerous and understudied issue in Albania. In part, this finding may be due to unresolved questions about definitions and a low threat perception based on an understanding of terrorism that is shaped by physical violence. Local authorities must implement a comprehensive, action-oriented approach to prevent, protect and ensure preparedness to respond to cyber-attacks. Therefore, in this way, cities become essential components for achieving preparedness and sustainability at the local and national level.

These dynamics tend to hide the weaknesses already faced by local response systems to cyber-attacks that threaten the loss of public trust in authorities, disruption of essential services, interference in social, political and economic activity - and in the most severe expression - destruction or physical losses.

This report recommends that a comprehensive, action-oriented approach be made a priority for local structures and every institution operating at the local level to prevent, protect and prepare for cyber-attacks.

Regardless of policies at the national level, the classification of information related to critical physical infrastructure, citizens and services are the ones who are ultimately affected at

the local level. This is why cyber security measures must be implemented, improved and developed at this level to protect citizens and services.

It is not enough for Albania to transpose the European Union Acquis (Directive (EU) no. 2022/2555 (NIS 2)"; for a more effective response to the security challenges of networks and information systems, a comprehensive approach is necessary at state level and more widely at the international level, which will include the creation of minimum but at the same time high and sufficient capabilities with the aim of planning, information exchange, cooperation and joint security obligations for operators of critical information infrastructures and operators of important information infrastructures.

Recommendations

1. The need for an integrated approach, with the involvement of citizens and local actors (in addition to the central structures of national security) for national preparedness and awareness of the risk from cyber threats or attacks.
2. Reviewing the cyber threat profile/risk register, and making the list of threats public, through awareness campaigns that focus on citizens.
3. Undertaking in-depth studies and making public the data on the social, psychological, physical and economic impact that cyber-attacks have on the life and personal integrity of every citizen in the Republic of Albania.
4. Undertaking an analysis of cyber response capabilities to map resources and identify gaps especially at the local level.
5. Orientation of national policies for local preparedness against cyber-attacks, guiding the preparation of "intervention strategies in case of cyber-attacks".
6. Undertaking awareness initiatives and engaging Internet providers in discussing institutional responses to new threats coming through social networks.
7. Inclusion in the agenda of the Local Public Security Councils of discussing specific cases of threats and cyber-attacks to guarantee public order and the local governance of cities, neighborhoods and local communities.
8. Guaranteeing financial incentives for improving cyber stability against any threat;
9. Establishing, empowering a city-level cyber operational center that brings together relevant experts from the public, private sector, civil society and academia to monitor, prepare and respond to cyber threats. This center should include investments in the physical and mental health of ICT specialists and capacity building.
10. Improving contracting agreements (through state interventions for the preparation of clauses to protect the moral integrity and life of users) to encourage investments by private operators to protect the most vulnerable groups of society such as children.
11. Synchronizing strategies to formalize an action-oriented integrated cybersecurity framework. This should take into consideration the development of sound policies and procedures for the inclusion of cyber security improvements in the infrastructure development life cycle of local structures.

12	Local and central planning of investment needs, based on the expected consequences resulting from the mapping of cyber threats that can affect critical infrastructure and services, and reducing the "cascade" effect of the spread of attacks.
13	Intensification of training and preparedness exercises in case of attacks as part of a coordinated program using "live-fire" exercises at all levels (national, regional and local multi-agency exercises).
14	Promotion of the basic principles of cyber "hygiene" and cyber security and their implementation as compulsory subjects in education. General cyber security communication and awareness campaigns should also be pushed into the public domain.
15	Sharing of experience and expertise and a proactive approach to building strategic partnerships to strengthen cyber capabilities against current and emerging threats

SIGURIA KIBERNETIKE DHE PËRGJIGJET SHUMËAKTORIALE NDAJ KËRCËNIMEVE DHE TERRORIZMIT KIBERNETIK

Përmbledhje praktikash dhe legjislacioni

2024