Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Transnational mechanisms for combating cyberterrorism in the context of digital transformation

Shermat OCHILOV [1]

Tashkent State University of Law

ARTICLE INFO

Article history:
Received September 2024
Received in revised form
15 October 2024
Accepted 25 October 2024
Available online
25 December 2024

Keywords:
cyberterrorism,
international cooperation,
UN,
international security,
digital transformation.

ABSTRACT

The article examines transnational mechanisms for combating cyberterrorism in the era of digital transformation. It explores the implementation of programs and initiatives adopted by international organizations, with a focus on resolutions, conventions, and other legal documents established within the framework of the United Nations. The roles of international entities such as NATO and the European Union in addressing cyberterrorism are also analyzed. The article proposes measures to enhance international cooperation in combating cyberterrorism. Specifically, it offers recommendations on the international legal classification of cyberterrorism, the adoption of a unified international framework, the creation of a centralized data exchange center, and the enhancement of mechanisms for international legal collaboration.

2181-1415/© 2024 in Science LLC.
DOI: https://doi.org/10.47689/2181-1415-vol5-iss11/S-pp51-63

Рақамли трансформация шароитида кибертерроризмга қарши курашнинг трансмиллий механизмлари

Kalit so‘zlar:
кибертерроризм,
халқаро ҳамкорлик,
БМТ,
халқаро хавфсизлик,
рақамли трансформация.

ANNOTATSIYA

Мақолада рақамли трансформация шароитида кибертерроризмга қарши курашнинг трансмиллий механизмлари таҳлил этилган. Халқаро ташкилотлар томонидан қабул қилинган дастурлар ва ташаббусларнинг имплементацияси хусусиятлари ўрганилган. БМТ доирасида қабул қилинган резолюциялар, конвенциялар ва бошқа норматив-ҳуқуқий ҳужжатлар таҳлил қилинган. Шунингдек, НАТО, Европа Иттифоқи каби халқаро

[1] Independent Researcher, Tashkent State University of Law. E-mail: ochilov.shermat00@mail.ru.

ташкилотларнинг кибертерроризмга қарши кураш соҳасидаги фаолияти тадқиқ этилган. Кибертерроризмга қарши курашда халқаро ҳамкорликни такомиллаштириш бўйича таклифлар ишлаб чиқилган. Хусусан, кибертерроризмнинг халқаро-ҳуқуқий квалификацияси, ягона халқаро ҳужжат қабул қилиш, маълумотлар алмашиш маркази ташкил этиш, халқаро ҳуқуқий ҳамкорлик механизмларини такомиллаштириш бўйича тавсиялар берилган.

Транснациональные механизмы борьбы с кибертерроризмом в условиях цифровой трансформации

Ключевые слова:
кибертерроризм,
международное
сотрудничество,
ООН,
международная
безопасность,
цифровая трансформация.

АННОТАЦИЯ

В статье рассматриваются транснациональные механизмы борьбы с кибертерроризмом в условиях цифровой трансформации. Изучены особенности реализации программ и инициатив, разработанных международными организациями. Проведен анализ резолюций, конвенций и других нормативно-правовых документов, принятых в рамках ООН. Также исследована деятельность таких международных организаций, как НАТО и Европейский Союз, в сфере борьбы с кибертерроризмом. Разработаны предложения по совершенствованию международного сотрудничества в данной области. В частности, даны рекомендации по международно-правовой квалификации кибертерроризма, принятию единого международного документа, созданию центра обмена данными и улучшению механизмов международного правового взаимодействия.

Дунёда жадал ривожланиб бораётган глобаллашув жараёнида замонавий ахборот-коммуникация технологиялари (АКТ) инсонлар учун қулайлик яратиш билан бир қаторда, инсоният учун хавфли жиноятлар ва турли таҳдидларни пайдо бўлишига ҳам имконият яратмоқда. Хусусан, терроризм, терроризмни молиялаштиришни янги шакллари ва сўнги йилларда анча ривожланиб борётган шунингдек, ўз ечимини кутаётган кибертерроризм каби халқаро ҳараткердаги жиноятлардир. БМТ Бош котиби Антонио Гутерриш таъкидлаганидек терроризмга қарши кураш виртуал макон ва ижтимоий тармоқларга ўтди, чунки, турли террористик ташкилотлар томонидан интернет кодланган хабарлар орқали музокаралар, “ёлланма аскарларни” ёллашга турли ташвиқот-тарғиботлар, ва бошқа жиноий ҳаракатларни мувофиқлаштириш учун фаол фойдаланиланишмоқда [1]. Статистик маълумотларга кўра, кибержиноятчилик бутун дунё бўйлаб компанияларга 2025-йилга келиб ҳар йили тахминан 10,5 триллион доллар зарар келтирди [2]. Шу билан бир қаторда кибертерроризмга қарши кураш воситаларининг глобал бозори 2023 ва 2030-йиллар оралиғида сезиларли суръатларда ўсиши кутилмоқда. Кибертерроризмни олдини олиш билан боғлиқ халқаро ҳуқуқий тартибга солиш борасида халқаро ҳуқуқда

универсал халқаро ҳужжат ҳанузгача мавжуд эмас. Ва ўз навбатида кибертерроризм орқали террористик ҳужумларни режалаштириш ва ташкил этишда айбдор шахсларни аниқлаш, уларни адолатли жиноий жавобгарликка тортиш, бу жиноятга қарши курашда халқаро ташкилотлар томонидан ишлаб чиқиладиган турли дастурлар, стратегиялар, тавсиялар давлатлар ўртасидаги икки томонлама ҳамкорлик дастурлари ва ҳуқуқни муҳофаза қилувчи органлар ҳамкорлиги, давлатлар миллий қонунчилигида бу жиноятга қарши кураш бўйича аниқ механизмларни такомиллаштириш долзарб аҳамият касб этмоқда.

Бугунги кунда ривожланиб бораётга глобал тармоқ кибержиноятнинг энг хавфли турларидан бири – кибертерроризм анъанавий терроризм билан таққослаганда, террорчилик ҳаракатларини фан ва техниканинг сўнги ютуқларига мурожаат этган ҳолда амалга оширишдир. Кибертерроризмнинг хавфлилик даражасини Ўзбекистон Республикаси Президенти Ш.Мирзиёев шундай таъкидлайди, “бугун дунёнинг деярли барча мамлакатлари кибермакондаги терроризм билан тўқнашмоқда. Интернет радикал ғояларни тарқатиш, одамларни ёллаш, террорчилик ҳаракатларини молиявий таъминлаш, режалаштириш ва содир этиш воситасига айланмоқда” [3]. Шу боисдан бугунги кунда кибержиноятларни пайдо бўлишининг назарий асослари, кибер жиноят ва кибертерроризмнинг ҳуқуқий тушунчаларини ишлаб чиқиш, кибертерроризмга қарши курашда халқаро ва минтақавий ташкилотларда такомиллаштириш, кибертерроризм қарши курашда давлатлар ҳамкорлигини ривожлантириш ўз навбатида мазкур муаммо доирасида илмий тадқиқотларнинг устувор амалга оширилишини талаб этмоқда. Габриел Вейманн (Габриел Weиманн) кибертарроизмни бугунги кунда глобал хавфсизликка жиддий таҳдидини шундай таъкидлайди, "кибертаррористлар нафақат информацоин технологиялар инфратузилмасига зарар етказиш, балки жамиятда қўрқув ва ваҳима уйғотиш мақсадида ҳам фаолият кўрсатмоқда" [4]. Бу эса ўз навбатида, халқаро ҳамжамиятдан янада кенг кўламли ва самарали чоралар кўришни талаб қилади.

Шуни таъкидлаш керакки, кибертерроризмга қарши курашда давлатларнинг халқаро ҳуқуқий ҳамкорлиги масалалари ҳозирча универсал даражада ҳал қилинмаган. Шундай бўлса-да кибертерроризмнинг айрим масалалари минтақавий ва универсал халқаро ҳужжатларда акс эттирилди. Универсал тартибда халқаро ҳужжатнинг қабул қилинмаганлиги натижасида бугунги кунда кибертерроризмни бевосита халқаро ҳарактердаги жиноятлар таркибида санаб ўтишга бир қанча ҳуқуқшнослар томонидан ҳақли эътирозлар [5] ҳам билдириб келинмоқда.

Н.Морозовнинг ҳақли эътирозини давом эттириб шуни қайд этишимиз керакки, бундай жиноят таркиби, унинг элементлари борасида умумий тушунча мавжуд эмас. Шунингдек, халқаро шартномаларда кибертерроризм актларига қарши курашда давлатларнинг ваколатли органлари ўртасидаги ўзаро муносабатларнинг процессуал шакллари ҳам тартибга солинмаганлигидадир. Шундай бўлсада, агар кибертеррозимнинг айрим жиноий ҳаракатлари 2000-йил 15-ноябрда БМТ томонидан қабул қилинган “Трансмиллий уюшган жиноятчиликка қарши” Конвенсиясининг [6] 3-моддаси талабларига жавоб берса уни халқаро ҳарактердаги жиноят сифатида кўриб чиқиш мумкин ҳисобланади. Яъни кибертерроризм ҳаракатлари халқаро тинчлик ва хавфсизликка таҳдид

сифатида баҳоланса уни халқаро трансмиллий жиноят сифатида квалификация қилиш мумкин деб ҳисоблаймиз.

Бундан ташқари, кибертерроризм халқаро тинчлик ва хавфсизликдан ташқари оммавий тартибда инсонлар ўлим учун ҳақиқий таҳдидларни келтириб чиқариши билан бугунги кунда хавфли ҳисобланади. Мисол учун 2010-йилда Эрон ядровий дастурини ёқ қилишга қаратилган “Стухнет” вируси бутун дунё бўйлаб аҳоли, қўшни давлатлар ва бошқа мамлакатлар учун потенциал хавфли оқибатларга олиб келиши мумкин эди [7]. Ушбу вируснинг тарқалиши бир неча мамлакатларда, шу жумладан АҚШ, Индонезия, Ҳиндистон, Озарбайжон, Покистон ва бошқаларда коммунал хизматларни бошқаришга мулжалланган компютер тармоқларига ҳам таъсир кўрсатган [8].

Бугунги кунга келиб БМТ халқаро терроризмга қарши курашиш бўйича ўн тўртта Конвенция қабул қилди ва уларга тўртта ўзгартириш киритди. Лекин, БМТ киберхавфсизлик масаласида фақат чекланган ҳаракатларни амалга ошириб келмоқда. Мисол учун, БМТ Бош Ассамблеяси томонидан бир нечта тегишли резолюцияларни келтиришимиз мумкин [9]. Ушбу қабул қилинган резолюцияларда бевосита халқаро хавфсизликни сақлашда ахборотлаштириш ва телекоммуникация ютуқларига бағишланганлигини кўришимиз мумкин.

Бирлашган Миллатлар Ташкилоти Бош Ассамблеясининг 2000-йил 4-декабрда қабул қилинган резолюциясида [10] давлатлар ахборот технологияларидан жиноий фаолиятдан фойдаланишга қарши курашишнинг турли усуллари кўриб чиқилди. Шунингдек, 2002-йилда Бош Ассамблеянинг 57/239-сон резолюцияси [11] қабул қилинди. Ушбу резолюция билан глобал киберхавфсизлик маданиятини яратиш белгилаб берилди. Резолюция глобал киберхавфсизлик маданияти яратишда барча иштирокчи давлатлардан қуйидаги тўққизта қўшимча элементни ҳисобга олишни талаб қилади. Булар, хабардорлик, маъсулият, жавобгарлик, этика, демократик, таҳдидларни баҳолаш, хавфсизлик тизимини ишлаб чиқиш ва жорий этиш, хавфсизликни бошқариш ва қайта баҳолаш кабилар.

Бош Ассамблеянинг 2014-йилда қабул қилинган 68/276-сон резолюцияси қабул қилингандан сўнг, Бош Ассамблеянинг кейинги резолюциялари давлатлар томонидан тезкорлик билан кибертеррорчилик фаолиятига қарши курашиш чораларини кўриш зарурлигини таъкидлаб, интернетдаги террорчилик фаолиятларининг кучайишини ва терроризмнинг кўпайишини олдини олиш бўйича чоралар кўриш муҳимлигини таъкидланди.

БМТ Бош Ассамблеяси каби БМТнинг Хавфсизлик Кенгаши халқаро тинчлик ва хавфсизликни сақлашга маъсул бўлган асосий органлардан биридир [12]. Бугунги кунгача Хавфсизлик Кенгаши терроризмга қарши кураш бўйича бир қанча резолюциялар қабул қилди. Мазкур резолюциялар таркибида албатта кибержиноятлар ва кибертерроризмга қарши курашни тартибга солувчи айрим резолюцияларни таҳлил этиш муҳимдир. Хусусан 2005-йилда Хавфсизлик Кенгаши халқаро чегаралар хавфсизлиги соҳасида халқаро ҳамкорликни мустаҳкамлашга қаратилган 1624-сонли резолюцияни қабул қилди. Ушбу резолюция орқали Хавфсизлик Кенгаши “барча давлатларни қуйидагиларга чақирувчи” террорчилик ҳаракатларига даъват этишни қоралади:

- террорчилик хатти-ҳаракатлари содир этишга ундашни қонун билан тақиқлаш;
- ушбу хатти-ҳаракатларнинг олдини олиш;
- террористик ҳаракатларда иштирок этган ва ушбу ҳаркатлар ҳақида ишончли ва тегишли маълумотларга эга бўлган ҳар қандай шахсга бошпана беришдан бош тортиш [13]. 1624-сонли резолюция Хавфсизлик Кенгашининг кибертерроризм фаолиятига қарши курашиш бўйича муҳим қадам бўлиб хизмат қилди.

Хавфсизлик Кенгашининг интернетдан фойдаланиб кибертерроризмга қарши кураш бўйича саъй-ҳаракатлари 2013-йилда ИШИД томонидан ижтимоий тармоқ платформаларидан фойдаланган ҳолда онлайн террорчилик кампаниясини бошлаганида кучайишни бошлади. Натижада Хавфсизлик Кенгаши томонидан 2013-йилда 2129-сонли Резолюция қабул қилинди. Ушбу резолюцияга кўра: “терроризм ва ахборот-коммуникация технологиялари, хусусан, Интернет тармоғидан, алоқа ўрнатиб ва бундай алоқалардан фойдаланиб ахборот-технологиялар орқали террористик ҳаракатларни қўзғатиш, уларни жалб қилиш, молиялаштириш, режалаштириш орқали террористик ҳаракатларни содир этиш ва уларга ёрдам бериш [14]” деб аниқ кибертерроризмнинг содир этилишига қарши курашни тақиқлашга чақирилди. Ушбу резолюция орқали Хавфсизлик Кангаши интернетдан фойдаланиш ва терроризм ўртасидаги боғлиқлик ортиб бораётганини “қайд этди”. Аммо ушбу резолюцияда кибертерроризмга қарши курашда давлат томонидан чора кўриш талаби мавжуд эмас. Шундай бўлсада Хавфсизлик Кенгаши барча давлатларни интернетдан террористик мақсадларда фойдаланиш тобора ривожланиб бораётганлигидан огоҳлантиришга эришди. 2129-сон резолюцияга кўра, Хавфсизлик Кенгашининг Аксилтеррор қўмитаси Ижроия директори БМТга аъзо давлатлар, халқаро, минтақавий ва субминтақавий ташкилотлар, шунингдек хусусий скетор вакиллари ва фуқаролик жамиятларининг бошқа институтлардан ҳамкорликда тероррчилик фаолиятида ахборот-комуникация технологиялари фойдаланишни олдини олиш ва унга қарши кураш бўйича қўмита томонидан доимий таклифлар, турли консептуал ёндашувлар олиб боришлиги белгилаб қўйилди.

Кибертерроризм фаолияти бевосита 2014-йилда қабул қилинган 2133-сонли резолюцияда янада тўлиқ таъкидланди. Резолюцияга кўра, ҳар қандай терроризмни молиялаштириш террорчиларни ёллаш бўйича саъй-ҳаракатларни қўллаб-қувватловчи муҳим жиноий ҳаракат ҳисобланади ва аъзо давлатлар терроризмни молиялаштиришга қарши кураш чоралари амалга ошириши кераклиги белгиланди.

Айнан мазкур йилда қабул қилинган Хавфсизлик Кенгашининг 2178-сонли резолюцияси [15] билан “а’зо давлатлар террорчиларнинг террористик ҳаракатларни қўллаб-қувватлашга ундаш учун ахборот-технология, алоқа ва электрон ресурслардан фойдаланишига ёл қўймаслик учун миллий чораларни кўришда биргаликда ҳаракат қилиш”га чақирилди. Юқорида қабул қилинган резолюциялар қаторида Хавфсизлик Кенгаши кибертеррорризмга қарши кураш бўйича 2016-йилда 2322-сон [16] резолюция, 2016-йилда 2331-сон [17] резолюция, 2017-йилда 2341-сон [18] резолюция ва 2017-йилда 2396-сон [19] резолюциялар қабул қилди. Ушбу резолюцияларда Хавфсизлик Кенгаши давлатларни рақамли

далилларни тўплаш ва сақлашга чақиради. Натижада рақамли далиллар орқали терговлар ўтказилиши ва террористик ҳужумларда айбдорларга нисбатан адолатли жавобгарликни белгилаш мумкинлиги белгиланди.

Хавфсизлик Кенгашининг 2019-йилда қабул қилимган 2469-сон [20] резолютисяси орқали террорчилик мақсадларида маблағ йиғиш учун турли электрон тўлов платформаларидан фойдаланиш, шунингдек, бундай маблағларни кўчириш ва ўтказиш учун олдиндан тўланган карталар ва мобил тўловлар ёки виртуал активлар каби янги тўлов усулларидан фойдаланишни олдини олиш ва бундай ҳаракатларни амалга оширган шахсларга нисбатан жавобгарликни белгилаш мақсадида давлатлар ўртасида ҳамкорликни ривожлантириш талаб этилди.

Шунингдек, террористик мақсадларда энг янги коммуникация технологияларидан фойдаланишга қарши кураш, Бирлашган Миллатлар Ташкилоти Хавфсизлик Кенгашининг Терроризмга қарши кураш қўмитасининг 2022-йил 28-29-октябр кунлари Ню-Деҳлида бўлиб ўтган махсус йиғилишида муҳокама қилинди ва барча учун мажбурий аҳамиятга эга бўлмаган Деҳли декларацияси [21] қабул қилинди. Деҳли декларациясига кўра Терроризмга қарши кураш қўмитаси “глобаллашган жамиятда террорчилар ва уларнинг тарафдорлари томонидан Интернет ва бошқа ахборот-коммуникация технологияларидан, жумладан ижтимоий тармоқ платформаларидан террористик мақсадларда фойдаланиш кенгайиб бораётганини ташвиш билан қайд этди”, энг янги технологиялардан - уларнинг қўлланилиши кенгайиб борган сари - террористик мақсадларда фойдаланишнинг олдини олиш, шунингдек бундай фойдаланишга қарши курашиш ўртасида мувозанатни таъминлаш зарурлигини" тан олди. Бунда "глобал рақамли алоқани ва эркин, ишончли ахборот оқимини сақлаб қолиш зарурлиги"га алоҳида эътибор қаратилди, чунки бу "иқтисодий ривожланиш, коммуникация, иштирок этиш ва ахборотга киришга ёрдам беради".

БМТ асосий органлари томонидан қабул қилинган узоқ йилга мўлжалланган стратегиялар, дастурлар, тавсиялар ва резолюциялар қаторидан ўз навбатида замонавий дунёда ривожланиб бораётган ва ҳали ўз ечимини топишга улгурмаган кибержиноятлар яъни кибертерроримга қарши курашни ўзида акс эттирган **«Киббертерроризмни олдини олиш ва унга қарши кураш тўғрисида»**ги Конвенция ва **«Криптовалюталар ва бошқа янги технологиялар орқали терроризмни молиялаштиришга қарши кураш тўғрисида»**ги Конвенциялар қабул қилиш давр талаби бўлиб қолмоқда. «Киббертерроризмни олдини олиш ва унга қарши кураш тўғрисида»ги Конвенция террористик гуруҳлар томонидан киберҳужумларни тарғиб қилиш, киберҳужумларга содир этишга ёллаш, тарғиб қилиш, кибер макон орқали турли террористик ҳаракатларни молиялаштириш учун маблағ йиғиш ва кибермакон орқали инсонларни қўрқитиш, уларни қарам қилиб қўйиш, шахсларнинг шахсий маълумотларни ўзлаштириш ва улардан кенг фойдаланиш каби жиноий таҳдидлар ва ҳаракатларга қарши курашиш учун ҳуқуқий асос яратиши мумкин.

«Криптовалюталар ва бошқа янги технологиялар орқали терроризмни молиялаштиришга қарши кураш тўғрисида»ги Конвенция молиявий технологиялар ва крипто-валюталарнинг ривожланишини ҳисобга олган ҳолда, ушбу Конвенция терроризмни молиялаштириш учун бундай технологиялардан

фойдаланишга қарши курашиш учун халқаро стандартларни ўрнатиши ва бундай операцияларни аниқлаш ва олдини олиш учун ахборот алмашиш ва технологик ечимларни ишлаб чиқиш бўйича халқаро ҳамкорликни кучайтиради деб ҳисоблаймиз.

БМТнинг ихтисослашган органи бу Женевада жойлашган Халқаро телекомуникация Иттифоқи ҳисобланади. Ушбу ташкилот 2006-йил май ойида 2005-йилда Тунисда ўтазилган Ахборот жамияти бўйича бутунжаҳон саммитнинг давоми сифатида Глобал киберхавфсизлик бўйича ҳамкорликни ривожлантириш учун маслаҳатлашув тадбирини ташкил этди. Бу Ахборот жамияти бўйича бутунжаҳон саммити фаолиятининг С5 ёналиши бўйича мувофиқлаштирувчи йиғилиш эди ва бу йиғилишда АКТдан фойдаланишда ишонч ва хавфсизликни мустаҳкамлаш масалалари мйҳожкама этилди.

Ушбу йиғилишда киберхавфсизликни янада ошириш учун учта устувор ёналиш белгиланди. Биринчи устувор ёналиш давлатлар ўртасида, хусусан, киберхавфсизлик ва муҳим ахборот инфратузилмасини ҳимоя қилиш сиёсати тўғрисида маълумот алмашишни ўз ичига олади. Иккинчи устувор ёналиш миллий ҳуқуқий ёндашувларни уйғунлаштириш ва кибержиноятчилик соҳасидаги халқаро ҳуқуқий нормаларни мувофиқлаштиришни ўз ичига олади. Бунда кибер жиноятчиликка қарши курашнинг асосий халқаро ҳуқуқий стандартлари ва тамойилларини миллий қонунчиликка жорий этиш глобал киберхавфсизликни таъминлашда муҳим аҳамиятга эга. Учинчи устувор ёналиш киберхавфсизликни таъминлаш билан боғлиқ ҳодисаларни кузатиш, кибертаҳдидлар тўғрисида огоҳлантириш ва уларга жавоб бериш имкониятларини ривожлантиришни ўз ичига олади.

Халқаро ҳуқуқда БМТ ва унинг ихтисослашган ташкилотларидан ташқари яна бир нечта халқаро ташкилотлар киберхавсизликни таъминлаш ва кибержиноятларнинг барча турларига қарши курашни амалга ошириб келмоқда. Хусусан, Шимолий Атлантика шартномавий ташкилоти (кейинги ўринларда НАТО) киберҳужумларга қарши курашни бошлаганига у қадар узоқ вақтни қамраб олмайди. 2007-йилда Эстонияга қилинган киберҳужум НАТО ташкилотининг кибержиноятларга қарши кураш бўйича “кибернетик таълимот ва кенг қамровли кибернетик стратегияга эга эмаслигини” ва кўрсатиб қўйди [22]. Эстонияга қилинган ҳужумдан кейин НАТО дарҳол киберҳужумларни олдини олиш ва кибержиноятларга қарши курашни ташкил этиш мақсадида ўзининг биринчи йиғилишини — 2008-йилги Бухарест саммитини ўтказди. Ушбу саммит НАТОнинг киберҳужумларга ихтисослашган иккита янги бўлинмасини яратишга туртки бўлди: Киберхавфсизликни бошқариш бошқармаси ва Қўшма киберҳужум амалиётларини таҳлил этиш маркази.

Киберхавфсизликни бошқариш бошқармаси НАТО аъзолари ўртасида кибер мудофаа имкониятларини марказлаштиришга қаратилган. Кибержиноятлар ҳақида жуда кам маълумотларга эга бўлишига қарамай, бошқарма “таҳдидларни аниқ аниқлаш ва қисқа вақт ичидаа муҳим кибер разведкани амалга ошириш, қисқа вақт ичидаа электрон мониторинг қобилияти амалга ошириш” эришди натижада – Киберхавфсизлиги операцион марказига айлантирилди [23]. Қўшма киберҳужум амалиётларини таҳлил этиш маркази “НАТОнинг узоқ муддатли

киберхавфсизлик доктринаси ва стратегиясини ишлаб чиқишга кўмаклашиш”ни мақсад қилган.

Бундан ташқари, халқаро ташкилотлар каби каби айрим халқаро даражадаги давлатлар гуруҳлари томонидан ҳам кибертерроризмга қарши кураш бўйича салмоқли ишлар амалга оширилди. Хусусан, 1997-йилда Г8 давлатлари гуруҳи юқори технологияли жиноятчиликка қарши кураш бўйича кичик гуруҳни ташкил этди ва компютер жиноятларига қарши курашнинг ўнта тамойилини ишлаб чиқди ва қабул қилди. Бундан кўзланган асосий мақсад жиноят содир этган ҳар қандай шахс дунёнинг ҳеч бир жойида “хавфсиз бошпана” олмаслиги эди. Г8 давлатлари гуруҳ билан 40 ортиқ давлат ҳамкорлик қилишни ёқлаб чиқишди ва гуруҳ томонидан 24/7 хизмат кўрсатиш тармоғи ишлаб чиқилди. Бу тармоқ орқали кибержиноятчилик ва терроризмга қарши курашда 40 га яқин иштирокчи давлатлар ўртасида кибер фазони тергов қилиш ва электрон далилларни сақлашда самарали ёрдам берди. 2004-йилда “Катта саккизлик” давлатлар гуруҳининг Адлия ва Ички ишлар вазирлари йиғилишида қабул қилинган қўшма қарорда “давлатлар террорчиларга ва интернет орқали содир этиладиган жиноятларга қарши курашишда, барча мамлакатлар жиноят қонунчилигини такомиллаштиришни давом эттиришлари кераклиги белгиланди”.

2006-йилда Россия Федерациясида бўлиб ўтган “Катта саккизлик” давлатларининг Адлия ва Ички ишлар вазирлари терроризм, кибержиноятчилик ва кибер макон муаммоларига қарши курашиш, бундай жиноий ҳаракатларга нисбатан самарали қарши чораларини такомиллаштириш зарурлиги масалалари муҳокама этилди. Ва 2006-йилда Санкт-Петербург декларацияси қабул қилинди. Декларацияга кўра барча аъзо давлатлар учун терроризмга қарши кураш соҳасида халқаро ҳуқуқий базани жорий этиш ва такомиллаштириш мажбурияти тасдиқланди [24].

Айрим мутахассислар томонидан кибертерроризм актлари халқаро жиноятлар сифатида квалификация қилиш керак деб фикр билдиришади [5]. Чунки мутахассис кибертерроризм бевосита хавфсизлик ва тинчликка таҳдид сифатида баҳоланиши билан боғлиқлигини таъкидлайди. Кибертерроризмни халқаро жиноят сифатида квалификация қилиш мумкинлиги борасида Халқаро жиноят суди Низомида белгиланганлиши керакми? Халқаро жиноят суди 1998-йилда 120 та давлат томонидан Римда бўлиб ўтган конференцияда ташкил этилган. Халқаро жиноят судининг Рим статути қабул қилинди ва 2002-йил 1-июлда кучга кирди. Халқаро жиноят суди (ИСС) тарихдаги биринчи доимий, халқаро шартномаларга асосланган, тўлиқ мустақил халқаро жиноят суди бўлиб, қонун устуворлигини тарғиб қилиш ва энг оғир халқаро жиноятлар жазосиз қолмаслигини таъминлаш учун ташкил этилган. Суд миллий судларни алоҳида суд тизими ҳисобланади ва унинг юрисдиксияси фақат миллий жиноий юрисдиксияларини тўлдиришга ҳам хизмат қилади. Шунингдек, Халқаро жиноят судининг юрисдикцияси Рим Статутида белгилаб қўйилди ва шу билан бир қаторда суд давлатлар билан тергов ва жиноий жавобгарликка тортишда ҳамкорликни амалга ошириши ҳам мумкин.

Рим Статутининг 5-моддасида бевосита халқаро жиноятларнинг турлари аниқ санаб берилди. Аммо Рим Статутида терроризм жиноятлари каби бошқа оғир жиноятлар киритилмаган. Бугунги кунда Рим Статутига терроризм жиноятлари

халқаро жиноятлар сифатида киритиш бўйича таклиф тавсиялар ишлаб чиқилмоқда. Агар терроризм жиноятлари халқаро жиноят сифатида тан олинса бунда албатта кибертерроризм ва кибержиноятлар киритиш мақсадга мувофиқ ҳисобланарди ва Халқаро жиноят судининг кибержиноятларга қарши курашда ролини кенгайтиришга хизмат қилади.

Аммо терроризм ёки кибертерроризмнинг Рим Статутида мавжуд эмаслиги бу Халқаро жиноят судининг бу жиноятларга қарши курашишда ҳеч қандай иштироки мавуд эмас дегани эмас. Яъни, Рим Статутининг 93-моддаси 10-қисмига кўра, “Суд сўров олгандан сўнг, суд юрисдикциясига кирадиган жиноятни ташкил этувчи ёки сўровчи давлатнинг миллий қонунчилигига биноан оғир жиноят сифатида белгиланган қилмишлар бўйича суд тергов ёки суд ишларини олиб борувчи давлат билан ҳамкорлик қилиши ва унга ёрдам бериши мумкин.” деб белгиланганлиги жуда муҳимдир. Бу норма орқали давлатларнинг ҳамкорлигини амалга ошириш бўйича 2007-йил май ойида Эстониядаги киберҳужумларга қарши курашиш бўйича амалиётни олишимиз мумкин унда давлат ва Халқаро жиноят судининг ҳамкорликни амалга ошириш ва халқаро жиноий суд иштирокчи давлатнинг илтимосига биноан ушбу иш бўйича тергов ёки суд ишларини олиб борганлигидан далолат беради.

Киберхавфсизликни таъминлашда ёки кибержиноятчиликка қарши курашда Европа Иттифоқи бугунги кунда бошқа минтақавий ташкилотлардан фақрли ўлароқ энг тўғри ёндашувни амалга ошириб келмоқда. Интернет ва бошқа компютер тармоқларидан фойдаланган ҳолда содир этилган жиноятларга қарши курашиш бўйича биринчи халқаро шартнома бўлган Европа Кенгашининг 2001-йилдаги “Кибержиноятчиликка қарши кураш тўғрисида”ги Будапешт конвенсияси [25] (кейинг ўринларда – Будапешт конвенцияси) “асосан миллий қонунчилик ва халқаро ҳамкорлик орқали жамиятни кибержиноятчиликдан ҳимоя қилишга қаратилган умумий сиёсатни" белгилаб берувчи халқаро конвенсия Европа Иттифоқи мамлакатларида кибержиноятларга қарши курашни тартибга солувчи ягона халқаро ҳужжат ҳисобланади. Будапешт конвенсияси мамлакатларнинг компютер маълумотлари ва тизимларининг махфийлиги, яхлитлиги ва мавжудлигига қарши жиноятлар, шунингдек, компютер воситаларидан фойдаланиб маълумотлар мазмуни ва муаллифлик ҳуқуқи ва турдош ҳуқуқларнинг бузилиши билан боғлиқ барча турдаги ҳуқуқбузарликларга қарши курашиш тартибини белгилайди. Будапешт конвенциясида кўзда тутилган ва компютер тизимларининг ишлашига рухсатсиз аралашувни олдини олишга қаратилган кўплаб чора-тадбирлар террорчилик жиноятларини содир этиш ёлида ўзига хос тўсиқ бўлиб хизмат қилади.

2006-йил 1-мартда Кибержиноятчилик тўғрисидаги конвецияга қўшимча протокол кучга кирди. Қўшимча протоколни ратификация қилган давлатлар ирқчи ва ксенофобик компютер тизимлари орқали материал, шунингдек, ирқсчилик йоки ксенофобия томонидан таҳдид ва ҳақорат тарқатишни жиноий жавобгарликка тортишлари шартлиги белгиланди. Конвенсия Интернет ва бошқа компютер тармоқлари орқали содир етилган жиноятлар бўйича биринчи халқаро шартномадир, хусусан муаллифлик ҳуқуқининг бузилиши, компютер билан боғлиқ фирибгарлик, болалар порнографияси, таҳдид жиноятлари ва тармоқ хавфсизлиги жиноятларини ўз ичига олади. Шунингдек, у компютер тармоқларини қидириш ва

қонуний ушлашга доир қатор ваколатлар ва процедураларни ўз ичига олади [26]. Унинг муқаддимасида келтирилган асосий мақсади жамиятни ҳимоя қилишга қаратилган умумий жиноят сиёсатини олиб боришдир. Шунингдек, кибержиноятларга доир тегишли қонунларни қабул қилиш ва жорий етиш орқали халқаро ҳамкорликни тарғиб етади.

Юқоридаги таҳлиллардан келиб чиқиб шуни қайд этишимиз керакки кибертерроризмга қарши курашиш учун халқаро даражада аниқ белгиланган ҳаракатлар дастурини ишлаб чиқиш керак. Бунда:

Биринчидан, кибертерроризмнинг халқаро ҳуқуқий квалификацияси аниқ белгиланиши талаб этилади. Яъни, кибертерроризм ҳаракатларини белгилаб берган давлатларнинг қонунчилик амалиётида турли хил ёндашувларни халқаро даражада бир хиллаштириш амалга ошириш керак.

Иккинчидан, кибертерроризм ҳаракатларини халқаро ҳарактердаги жиноят сифатида тан олиниши учун ягона кибертерроризмга қарши кураш бўйича халқаро ҳужжатни қабул қилиш лозим.

Учинчидан, халқаро майдонда кибертерроризм ҳодисаларига тезкор жавоб беришга ёрдам берадиган, кибер таҳдидлар тўғрисида аниқ ва тезкор маълумотлар алмашиш учун давлатлар ҳамкорлигида ягона маълумотлатни мувофиқлаштириш марказини ташкил этиш.

Тўртинчидан, кибертерроризм жиноятини содир этган шахсларни қўлга олиш, уларни тергов қилиш, адолатли жиноий жавобгарликка тортиш, шу жумладан экстрадиция ва кибертерроризм жинояти билан боғлиқ далиллар алмашинуви учун халқаро ҳуқуқий ҳамкорлик механизмларини ишлаб чиқиш.

Бешинчидан, киберҳужумларни олдиндан аниқлаш ва уни олдини олиш учун сунъий интеллект технологияларини ишлаб чиқиш ва бу технологияларни қўллаш бўйича халқаро ҳамкорликни кучайтириш зарур.

Шуниндек, рақамлаштириш даврида терроризмга қарши курашишда халқаро ташкилотлар ва давлатлараро дастурлар ва ташаббусларни қўллаб-қувватлашнинг асосий жиҳатларини қуйидагилар орқали қайд этиш мумкин:

Биринчидан, рақамлаштириш ҳам террористик таҳдид хусусиятига, ҳам унга қарши курашиш усулларига сезиларли таъсир кўрсатди. Бир томондан, террористик ташкилотлар ўз фаолиятини тарғиб қилиш, янги аъзоларни жалб қилиш, молиялаштириш ва мувофиқлаштириш учун янги технологиялардан фаол фойдаланаётган бўлса. Бошқа томондан, рақамли технологиялар ҳуқуқни муҳофаза қилиш органлари ва махсус хизматлар учун террористик фаолиятни кузатиш, таҳлил қилиш ва олдини олиш соҳасида янги имкониятлар очмоқда.

Иккинчидан, замонавий терроризм билан самарали курашиш турли давлатларнинг саъй-ҳаракатларини яқиндан халқаро ҳамкорлик ва мувофиқлаштириш талаб қилади. Мавжуд давлатлараро дастурлар ва ташаббуслар бундай ҳамкорлик учун асос яратиш билан бир қаторда, бир неча жиддий қийинчиликларга ҳам дуч келмоқда. Буларга сиёсий ва геосиёсий омиллар, ҳуқуқий ва юрисдиксия муаммолари, технологик ва инфратузилмавий тўсиқлар, шунингдек молиялаштириш ва ресурслар билан таъминлаш масалаларини олишимиз мумкин.

Учинчидан, терроризмга қарши курашда халқаро ҳамкорликнинг ҳуқуқий базасини рақамли давр реалликларига мослаштириб янада ривожлантириш зарур.

Кибертерроризм ва террористик мақсадларда сунъий интеллектдан фойдаланиш хусусиятларини ҳисобга олган ҳолда янги халқаро конвенсиялар ишлаб чиқиш, шунингдек миллий қонунчиликни уйғунлаштириш масаласига алоҳида эътибор қаратиш лозим.

Тўртинчидан, давлатлараро дастурлар самарадорлигини оширишда технологик ҳамкорликнинг ривожланиши ҳал қилувчи рол ўйнайди. Технологиялар алмашинуви учун халқаро платформалар яратиш, умумий стандартлар ва протоколлар ишлаб чиқиш, шунингдек илғор технологиялар соҳасида қўшма тадқиқот ва илмий изланишлар олиб бориш халқаро ҳамжамиятнинг терроризм билан курашиш салоҳиятини сезиларли даражада кучайтириши мумкин.

Бешинчидан, давлатлар ўртасида ахборот алмашиш ва таҳлилий ҳамкорлик механизмларини такомиллаштиришга алоҳида эътибор қаратиш лозим. Бу эса ўз навбатида реал вақт режимида оператив маълумотлар алмашинувининг ҳимояланган тизимларини яратиш, халқаро таҳлил марказларини ривожлантириш ва катта маълумотларни таҳлил қилишнинг илғор технологияларини жорий этиш террористик таҳдидларни аниқлаш ва олдини олиш самарадорлигини сезиларли даражада ошириши мумкин.

Олтинчидан, замонавий терроризм билан курашишда муваффақиятга эришишда кўп жиҳатдан хусусий сектор вакиллари ва фуқаролик жамияти институтларини ўз ичига олган кенг доирадаги манфаатдор томонларни бу жараёнга жалб қилиш мақсадга мувофиқдир. Давлат ва хусусий сектор ҳамкорлиги, технология компаниялари ва ижтимоий платформалар билан ҳамкорлик, шунингдек нодавлат ташкилотларни радикаллашувнинг олдини олиш дастурларига жалб қилиш терроризм билан курашишга комплекс ёндашувнинг муҳим элементларига айланмоқда.

Еттинчидан, халқаро ташкилотлар томонидан ва давлатлараро ишлаб чиқилган дастурлар ва ташаббусларнинг замонавий террористик таҳдидларнинг тез ўзгарувчан шаклларига мослашишни рағбатлантириш. Бу нафақат технологик инновацияларни, балки янги қийинчиликларга тезкор жавоб бера оладиган мослашувчан институционал механизмларни ривожлантиришни ҳам талаб қилади.

Хулоса қилиб айтганда, рақамлаштириш даврида терроризм билан курашиш халқаро ҳамжамият учун нафақат технологик, балки ахлоқий вазифа ҳамдир. Терроризм билан курашиш чораларининг самарадорлиги ва фуқароларнинг фундаментал ҳуқуқ ва эркинликларини ҳимоя қилиш ўртасидаги мувозанатни топиш давлатлараро дастурларни ишлаб чиқиш ва амалга оширишда асосий вазифалардан бири бўлиб қолмоқда. Фақат шу мувозанатга риоя қилинган тақдирдагина терроризм билан курашишдаги халқаро ҳамкорлик ҳақиқатан ҳам муваффақиятли ва узоқ муддатли истиқболда барқарор бўлиши мумкин.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. «Объединиться для противодействия терроризму» – комментарий Генерального секретаря о конференции Организации Объединенных Наций высокого уровня по борьбе с терроризмом 26 июня 2018 г. // Организация

Объединенных Наций [Электронный ресурс]. – https://www.un.org/sg/ru/content/sg/articles/2018-06-26/uniting-world-againstterrorism
2. Elektron resurs: https://www.embroker.com/blog/cyber-attack-statistics/ (Murojaat qilingan sana 10.02.2024 y)
3. Sh.Mirziyoyev Yuqori darajadagi “BMT Global aksilterror strategiyasini amalga oshirish bo‘yicha Qo‘shma harakatlar rejasi doirasida Markaziy Osiyo mamlakatlarining mintaqaviy hamkorligi” xalqaro konferensiyasi ishtirokchilariga Murojaati // https://yuz.uz/uz/news/yuqori-darajadagi-bmt-global-aksilterror-strategiyasini-amalga-oshirish-boyicha-qoshma-harakiy-osiyo-mamlakatlarining-mintaqaviy-hamkorligi-xalqaro-konferentsiyasi-ishtirokchilariga
4. Weimann, Gabriel. Terrorism in cyberspace: The next generation. Columbia University Press, 2015. p. 151.
5. Н.О.Мороз МЕЖДУНАРОДНО-ПРАВОВАЯ КВАЛИФИКАЦИЯ КИБЕРТЕРРОРИЗМА «ИСТОРИЧЕСКИЕ НАУКИ. ЮРИДИЧЕСКИЕ НАУКИ». 2016. Т. 2. № 2 (6) С.81
6. Конвенция Организации Объединенных Наций против транснациональной организованной преступности: //https://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml
7. Fildes, J. (Technology Reporter), (2010, September 23). Stuxnet worm 'targeted high-value Iranian assets, BBC News, Retrieved from http://www.bbc.co.uk/news/technology-11388018 accessed on 30 September 2012
8. Symantec, W32.Stuxnet. 17 September 2010. Retrieved from http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99. accessed on 30 September 2012
9. G.A. Res. 58/32, U.N. Doc. A/RES/58/32 (Dec. 8, 2003); G.A. Res. 59/61, U.N. Doc. A/RES/59/61 (Dec. 3, 2004); G.A. Res. 60/45, U.N. Doc. A/RES/60/45 (Jan. 6, 2006); G.A. Res. 61/54, U.N. Doc. A/RES/61/54 (Dec. 19, 2006); G.A. Res. 62/17, U.N. Doc. A/RES/62/17 (Jan. 8, 2008); G.A. Res. 63/37, U.N. Doc. ARES/63/37 (Jan. 9, 2009); G.A. Res. 64/25, U.N. Doc. A/RES/64/25 (Jan. 14, 2010).
10. Elektron resurs: Resolution adopted by the General Assembly Combating the criminal misuse of information technologies A/Res/55/63 // https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf
11. Elektron resurs: Resolution adopted by the General Assembly Creation of a global culture of cybersecurity A/RES/57/239 // https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf
12. Ian Johnstone, ‘Legislation and Adjudication in the UN Security Council: Bringing Down the Deliberative Deficit’, 102 Am. J. Int’l L. 275 (2008), at p. 283.
13. Resolution 1624 (2005) Adopted by the Security Council at its 5261st meeting, on 14 September 2005 S/RES/1624 of 14 September 2005 // http://unscr.com/en/resolutions/doc/1624
14. Резолюция 2129 (2013), принятая Советом Безопасности на его 7086-м заседании 17 декабря 2013 года S/RES/2129 (2013) // https://documents.un.org/doc/undoc/gen/n13/624/39/pdf/n1362439.pdf?token=eVVgLgU0wCEQoF1uzH&fe=true

15. Резолюция 2178 S/RES/2178 (2014) // https://documents.un.org/doc/undoc/gen/n14/548/01/pdf/n1454801.pdf?token=AJBEuviHtiNKQorSQx&fe=true
16. Резолюция 2322 (2016) S/RES/2322 // https://documents.un.org/doc/undoc/gen/n16/433/58/pdf/n1643358.pdf?token=Zo2OYZgnwIaxPhvzEr&fe=true
17. Резолюция 2331 S/RES/2331 (2016) // https://documents.un.org/doc/undoc/gen/n16/451/62/pdf/n1645162.pdf?token=YSQqZo5iHzjIqHP0jL&fe=true
18. Резолюция 2341 S/RES/2341 (2017) // https://documents.un.org/doc/undoc/gen/n17/038/61/pdf/n1703861.pdf?token=eRwyhR9iK0A9ZmFuu4&fe=true
19. Резолюция 2396 S/RES/2396 (2017) // https://documents.un.org/doc/undoc/gen/n17/460/27/pdf/n1746027.pdf?token=wKVEyDxs7iPCthC6fG&fe=true
20. Resolution 2469 S/RES/2469 (2019) // https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2469.pdf
21. Делийская декларация, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_special_meeting_ outcome_document.pdf
22. Rex B. Hughes, NATO and Cyber Defence: Mission Accomplished?, ATLANTISCH PERSPECTIEF, Apr. 2009, at 1, available at http://www.atlcom.nl/site/english/nieuws/wpcontent/Hughes.pdf.
23. Scott J. Shackelford, Estonia Two-and-aHalf Years Later: A Progress Report on Combating Cyber Attacks, J. INTERNET L. 5 (forthcoming), available at http://ssrn.com/abstract=1499849.
24. САФАРОВА Ш. Инсон ҳуқуқлари бўйича таълимни амалга оширишнинг шартномавий-ҳуқуқий манбалари // Юрист Ахборотномаси. – 2023. – Т. 3. – №. 4. – С. 89-95. // https://yuristjournal.uz/index.php/lawyer-herald/article/view/876
25. Council of Europe, ETS No. 185, Convention on Cybercrime, pmbl., Budapest (Nov. 23,2001), entered into force July 1, 2004, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
26. Рахманов, Ш. Трансформация внешней политики и внешнеполитических ориентиров Республики Узбекистан и таргетирование дипломатического права международных организаций. SDU University Bulletin: Social Sciences, [S.l.], v. 53, n. 2, p. 50-63, dec. 2020. ISSN 2709-2410. Available at: <https://journals.sdu.edu.kz/index.php/ss/article/view/326>.2024.doi:https://doi.org/10.47344/sdubss.v53i2.32139/am.03-23.091