



CYBER DIPLOMACY: HISTORY, PROBLEMS AND PROSPECTS

Shokhijakhon Toshpulatov

Doctor of Philosophy (PhD) in Political Science, Senior Lecturer

Tashkent State Law University

Tashkent, Uzbekistan

E-mail: sh.toshpulatov@tsul.uz

ABOUT ARTICLE

Key words: diplomacy, cyber diplomacy, cyberspace, cyberattacks, phishing, hacking, technological innovations, global cooperation, prospects

Received: 26.12.24

Accepted: 28.12.24

Published: 30.12.24

Abstract: This article analyzes the concept of cyber diplomacy, its origins and historical evolution, its main features, and the perspectives shaping this process. At the same time, the initial diplomatic practices, the impact of technological innovations, and the emergence of cyber diplomacy as a separate area of global cooperation are studied in detail. In addition, this article puts forward proposals on the main thematic areas, including the role of technology in cyber diplomacy, cyber threats and methods of preventing them, and the institutional frameworks guiding cyber diplomacy. The article also examines contemporary problems in cyber diplomacy in detail. In addition, aspects such as the consequences of cybercrime, the spread of disinformation, and the use of artificial intelligence for malicious purposes are also covered.

KIBER DIPLOMATIYA: TARIX, MUAMMOLAR VA ISTIQBOLLAR

Shohijahon Toshpo'lotov

Siyosiy fanlari bo'yicha falsafa doktori (PhD), katta o'qituvchi

Toshkent Davlat yuridik universiteti

Toshkent, O'zbekiston

E-mail: sh.toshpulatov@tsul.uz

MAQOLA HAQIDA

Kalit so'zlar: diplomatiya, kiber diplomatiya, kibermakon, kiberhujumlar, fishing, hakkerlik, texnologik innovatsiyalar, global hamkorlik, istiqbollar

Annotatsiya: Mazkur maqolada kiber diplomatiya tushunchasi, uning kelib chiqishi va tarixiy evolyutsiyasi, uning asosiy xususiyatlari hamda ushbu jarayonni

shakllantiruvchi istiqbollar tahlil qilingan. Shu bilan birga, dastlabki diplomatik amaliyotlar, texnologik innovatsiyalarning ta'siri va global hamkorlikning alohida sohasi sifatida kiberdiplomatiyaning paydo bo'lishi atroflicha o'rganilgan. Bundan tashqari ushbu maqolada kiber diplomatiyada texnologiyaning roli, kibertahdidlar va ularni oldini olish usullari hamda kiber diplomatiyaga rahbarlik qiluvchi institutsional asoslarni o'z ichiga olgan asosiy tematik yo'nalishlar bo'yicha takliflar ilgari suriladi. Shuningdek, maqolada kiber diplomatiyadagi zamonaviy muammolar atroflicha ko'rib chiqildi. Bundan tashqari, kiberjinoyatlarning oqibatlar, dezinformatsiyaning tarqalishi, sun'iy intellektdan g'arazli maqsadlarda foydalanish kabi jihatlar ham yoritilgan.

КИБЕРДИПЛОМАТИЯ: ИСТОРИЯ, ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Шоҳиджаҳон Тошпулатов

*Доктор философии (PhD) по специальности «Политология», старший преподаватель
Ташкентский государственный юридический университет*

Ташкент, Узбекистан

E-mail: sh.toshpulatov@tsul.uz

О СТАТЬЕ

Ключевые слова: дипломатия, кибердипломатия, киберпространство, кибератаки, фишинг, хакерство, технологические инновации, глобальное сотрудничество, перспективы

Аннотация: В статье анализируется концепция кибердипломатии, ее истоки и историческая эволюция, ее основные характеристики, а также перспективы, формирующие этот процесс. В то же время подробно рассматриваются ранняя дипломатическая практика, влияние технологических инноваций и становление кибердипломатии как отдельной области глобального сотрудничества. Кроме того, в статье выдвигаются предложения по ключевым тематическим направлениям, включая роль технологий в кибердипломатии, киберугрозы и методы их предотвращения, а также институциональные рамки, регулирующие кибердипломатию. В статье также всесторонне рассмотрены современные проблемы кибердипломатии. Кроме того, рассматриваются такие аспекты, как последствия киберпреступности, распространение дезинформации и использование искусственного интеллекта в вредоносных целях.

Kirish

Har bir davrda diplomatiya an'anaviy xabar almashinish vositalaridan tortib, zamonaviy raqamli platformalargacha mavjud vositalardan samarali foydalanishga harakat qilgan. Diplomatiyaning kelib chiqishi ham qadimiy tamaddun beshiklariga borib taqaladi, xususan, turli mamlakatlarning vakillari – ittifoqlar tuzish, savdo-sotiqni yanada rivojlantirish va tinchlik bitimlariga erishish yuzasidan muzokaralar olib borish uchun yuborilgani bunga yorqin misol. Shu bilan birga, aloqa texnologiyalari takomillashib borishi ham tadrijiy ravishda diplomatik amaliyotlarning jadallashuviga ijobiy ta'sir ko'rsatdi. Masalan:

–**Bosmaxonaning roli:** XV asrda Yohan Gutenbergning Germaniyada kitob bosish dastgohini ixtiro qilishi, dunyo bo'ylab axborotni tez tarqalishiga yo'l ochdi va diplomatlarga xalqaro voqealardan yaxshiroq va kengroq xabardor bo'lish imkonini berdi.

–**Telegraf inqilobi:** 1832-yilda P.L.Shillingning elektromagnit telegraf apparatini yaratishi poytaxtlar o'rtasida aloqa qilish uchun zarur bo'lgan vaqtni keskin qisqartirdi, hukumatlarning o'zaro munosabatlarini takomillashtirdi.

–**Telefon va radio:** 1876-yil A.G.Bellning telefonni va 1895-yil A.S.Popovning radioni ixtiro qilishi XX asr real vaqt rejimida aloqa vositalarining yuksalishini ta'minladi, bu esa o'z navbatida davlatlar o'rtasida samarali muloqot va tezkor koordinatsiya imkonini berdi.

Tarixdagi tub burilishlarga sabab bo'lgan bu o'zgarishlar, butun dunyoda aloqalar almashinuvi tizimini yangicha rakursga ko'tardi va kiberdiplomatiyaning paydo bo'lishiga tamal toshini qo'ygan (kvintessensiya rolini o'ynadi deyish mumkin) raqamli transformatsiya uchun asos yaratdi.

Raqamli dunyoning yuksalishi

Raqamli texnologiyalarning yuksalishi xalqaro munosabatlar manzarasini tubdan o'zgartirdi. Kiberdiplomatiya, kibermakonda yuzaga keladigan muammolarni hal qilish uchun diplomatik vositalar va jarayonlardan foydalanish global boshqaruvning muhim sohasiga aylandi. Rivojlanayotgan ushbu soha mojarolarni boshqarish, kelishuvlar bo'yicha muzokaralar olib borish va tobora o'zaro bog'langan kibermakonda hamkorlikni rivojlantirishga qaratilgan sa'y-harakatlarni o'z ichiga oladi.

Shu jihatdan kiber diplomatiya xalqaro munosabatlarni kibermakon orqali boshqarish amaliyoti bo'lib, raqamli infratuzilma, kiberxavfsizlik va virtual munosabatlarni tartibga solish masalalari orqali diplomatik faoliyatdagi sezilarli o'zgarishni ifodalaydi.

Kiberdiplomatiya – an'anaviy diplomatiyaning kibermakon sohasidagi kengaytmasi. U kiberjinoyat, raqamli maxfiylik, internet boshqaruvi va kiberxavfsizlik kabi muammolarni hal qilish uchun muzokaralar, konstruktiv muloqotlar va samarali hamkorlikdan foydalanishni ham o'z ichiga oladi.

Kiberdiplomatiyaning kelib chiqishini XX asr oxirlarida internetning rivojlanishi bilan bog'lash mumkin. Dastlab akademik va harbiy maqsadlar uchun tadqiqot vositasi sifatida yaratilgan internet tez orada global fenomenga aylandi. Uning asosiy bosqichlari quyidagilarda ko'rinadi:

–1960-yillar: AQSh Mudofaa vazirligi tomonidan ARPANETning yaratilishi bilan zamonaviy internetga asos solindi.

–1980-1990 yillar: Internetning tijoratlashuvi va World Wide Web (Jahon o'rgimchak to'ri)ning paydo bo'lishi bilan butun dunyo bo'ylab shaxslar va tashkilotlarning ulardan keng ko'lamda foydalanishiga olib keldi.

Internetga bo'lgan talabning o'sib borishi bilan, undan foydalanish bilan bog'liq xavflar ham ortib bordi. 1990-yillarning oxiri va 2000-yillarning boshlarida kiberhujumlar, ma'lumotlar bazalarining buzilishi va boshqa zararli harakatlar ko'paydi. Bu esa davlatlarni ushbu muammolarni hal qilish uchun xalqaro hamkorlik doirasida hal qilishlari zarurligini tan olishga undadi.

Tadqiqotning usullari:

–Kiberdiplomatiya tushunchasining mohiyati va kelib chiqishini aniqlashda, uning siyosiy va iqtisodiy ahamiyatini ochib berishda **analiz metodidan** foydalanildi. Ushbu metod orqali, maqolaning natijalar qismida tegishli global darajadagi kiberdiplomatiya strategiyalari analitikasini ko'rsatishga muvaffaq bo'lindi.

–Turli davlatlarning kiberdiplomatiya bo'yicha yondashuvlari va tajribalarini tahlil qilishda **qiyosiy-solishtirma metod**dan foydalanildi. Xususan, AQSh, Yevropa Ittifoqi va Xitoyning kibersiyosati o'rtasidagi farqlar solishtirildi.

–Kiberdiplomatiyaning kelib chiqishi va rivojlanishini aniqlash hamda ko'rsatib berish uchun, internetning paydo bo'lishidan tortib, xalqaro hamkorlikda foydalanishga qadar bo'lgan jarayonlar **tarixiy (retrospektiv) metod** orqali o'rganildi.

–Xalqaro tashkilotlar (masalan, BMT) tomonidan ishlab chiqilgan kiberxavfsizlik va internet boshqaruvi bo'yicha huquqiy asoslar **normativ-huquqiy tahlil metodi** orqali ko'rib chiqildi.

–Amaliy misollar orqali kiberdiplomatiyaning davlatlararo munosabatlarda qanday rol o'ynashini ko'rsatib berish uchun **empirik tadqiqot metodidan** foydalanildi.

Ushbu maqola doirasida quyidagi mualliflarning asarlari birlamchi manbalar hisoblanadi:

1. Samuel Josef Nayning "Yumshoq kuch"(Soft power) asari kiberdiplomatiyaning aynan "yumshoq kuch" bilan bog'liq jihatlarini o'rganishda asosiy manba sifatida foydalanildi.

Bundan tashqari Nayning yana bir **“Kiber kuch”(Cyber Power)** asari global darajadagi kiber siyosatni tushunishda muhim manba hisoblanadi.

2. **Devid P. Fidler** kiber diplomatiyaning xalqaro huquqiy jihatlarini tadqiq qilgan, ayniqsa, markaziy internet boshqaruvi va xalqaro hamkorlik masalalariga urg'u bergan.

3. **Timoti More** esa kiber diplomatiya va kiberxavfsizlikdagi davlatlar o'rtasidagi kelishmovchiliklarni yengillashtirishda xalqaro yondashuvlarni munosib darajada ko'rsatib bergan.

4. **Aleksandr Klimburgning "The Darkening Web"(Zulmatdagi to'r)** kitobi kiberxavfsizlik va kiberdiplomatiya bo'yicha dolzarb masalalarni ochib beradi.

5. **Budapesht Convention on Cybercrime (Kierjinoatlar bo'yicha Budapesht konvensiyasi)** - internet jinoyatchiligiga qarshi xalqaro huquqiy asos vazifasini o'tab kelmoqda.

6. **BMTning Group of Governmental Experts (Hukumat ekspertlari guruhi)** hisobotlari: Kiberdiplomatiya bo'yicha xalqaro hamkorlikni o'rnatish hamda bu borada davlatlararo tartibni belgilashda muhim ahamiyatga ega xalqaro hujjat hisoblanadi.

Natijalar:

Ushbu maqola yuzasidan quyidagi natijalarni ma'lum qilamiz:

Muammo	Tavsif	Statistika
Kiberhujumlar sonining oshishi	Davlatlar va nodavlat aktorlar tomonidan amalga oshirilayotgan kiberhujumlar soni ortib bormoqda, bu esa xalqaro munosabatlarda ziddiyatlarni kuchaytirmoqda.	2023-yilda kiberhujumlar soni 2022-yilga nisbatan 38% ga oshgan. Manba: https://www.accenture.com/us-en
Xalqaro huquq me'yorlarining bu borada noaniqligi	Kiberdiplomatiya sohasida xalqaro huquqiy me'yorlarning yetarli darajada rivojlanmaganligi davlatlar o'rtasida kelishmovchiliklarga olib kelmoqda.	2024-yilda o'tkazilgan so'rovnoma natijalariga ko'ra, diplomatlarning 65% i kibermakonni tartibga soluvchi xalqaro huquqiy me'yorlarning yetarli emasligini ta'kidlagan. Manba: https://carnegieendowment.org/?lang=en
O'zaro ishonchning yetishmasligi	Davlatlar o'rtasida kibermakondagi faoliyat bo'yicha ishonchning pastligi hamkorlikni qiyinlashtirmoqda.	2023-yilda o'tkazilgan xalqaro tadqiqotga ko'ra, respondentlarning 70% i boshqa davlatlarning kibermakondagi niyatlariga ishonchsizlik bildirgan. Manba: https://www.pewresearch.org/
Texnologik tafovutlar	Rivojlangan va rivojlanayotgan davlatlar o'rtasidagi texnologik imkoniyatlardagi	2024-yilgi ma'lumotlarga ko'ra, rivojlangan davlatlarda internetga kirish imkoniyati 90% dan yuqori bo'lsa, rivojlanayotgan davlatlarda bu ko'rsatkich 40% dan past. Manba:

	farqlar kiberdiplomatiyada tengsizlikka olib kelmoqda.	https://www.itu.int/ru/Pages/default.aspx#/ru
Kiberxavfsizlik sohasida kadrlarning yetishmasligi	Kiberdiplomatiya sohasida malakali mutaxassislarining yetishmasligi samarali siyosat yuritishni qiyinlashtirmoqda.	2023-yilda global miqyosda 3,5 million kiberxavfsizlik bo'yicha mutaxassis yetishmasligi qayd etilgan. Manba: https://cybersecurityventures.com/

Ushbu natijalar asosida quyidagi istiqbollarni ko'rsatish mumkin:

Istiqbollar	Tavsif	So'nggi yutuqlar
Kiberxavfsizka sarmoyalar kiritishning oshishi	Davlatlar va tashkilotlar kiberxavfsizlikni kuchaytirish uchun moliyaviy resurslarni ko'paytirmoqdalar.	2023-yilda global kiberxavfsizlik bozorining hajmi \$173,5 milliardga yetgan va 2028-yilga kelib \$270 milliarddan oshishi kutilmoqda. Manba: Statista https://www.statista.com/
Xalqaro kiber kelishuvlarning ko'payishi	Davlatlar o'rtasida kibermakonda hamkorlikni mustahkamlash uchun yangi xalqaro kelishuvlar va shartnomalar tuzilishi kutilmoqda.	2024-yilda BMT doirasida 15 ta yangi kiberxavfsizlik bo'yicha kelishuvlar imzolangan. Manba: United Nations https://www.un.org/en/
Kiber diplomatik missiyalarning kengayishi	Ko'proq davlatlar kiberdiplomatiya bo'yicha maxsus elchilar va bilimlarni tashkil etish orqali o'z diplomatik faoliyatlarini kengaytirmoqda.	2023-yilda 50 dan ortiq davlat kiberdiplomatiya bo'yicha maxsus elchilarni tayinlagan. Manba: Carnegie Endowment for International Peace https://carnegieendowment.org/?lang=en
Kiber tahdidlarga qarshi xalqaro hamkorlikning kuchayishi	Davlatlar va xalqaro tashkilotlar kiber tahdidlarga qarshi birgalikda kurashish uchun hamkorlikni kuchaytirmoqdalar.	2024-yilda NATO kiberxavfsizlik bo'yicha 10 ta qo'shma mashg'ulot o'tkazgan. Manba: NATO rasmiy sayti https://www.nato.int/cps/en/natohq/search.htm
Kiber diplomatiya bo'yicha ta'lim dasturlarining rivojlanishi	Universitetlar va ta'lim muassasalari kiberdiplomatiya bo'yicha maxsus dasturlarni joriy etish orqali mutaxassislar sonini ko'paytirmoqdalar.	2023-yilda 30 dan ortiq universitet kiberdiplomatiya bo'yicha magistratura dasturlarini taklif qilgan. Manba: University Programs in Cyber Diplomacy https://www.uel.ac.uk/postgraduate/courses/msc-cyber-diplomacy

Muhokama

Kiberdiplomatiyaning rivojlanishi

XX asrning oxirlarida kibermuammolarni diplomatik vositalar orqali hal qilish bo'yicha birinchi muhim sa'y-harakatlar boshlandi:

1. Kiberjinoyatlar bo'yicha Budapesht konvensiyasi (2001): Bu kiberjinoyatchilikka qarshi kurashga qaratilgan birinchi xalqaro shartnoma bo'lib, kiberjinoyatlarni yuridik malakalashning huquqiy asoslarni yaratish va hamkorlikni rivojlantirish uchun davlatlarni birlashtirdi.

2. Birlashgan Millatlar Tashkilotining ishtiroki: Birlashgan Millatlar Tashkiloti kiberxavfsizlikni tinchlik va xavfsizlik bo'yicha kengroq muhokamalar doirasida, jumladan, 2004 yilda Axborot xavfsizligi bo'yicha Hukumat ekspertlar guruhini (GGE) tashkil etish orqali hal qilishni boshladi.

–Amerika Qo'shma Shtatlari: Internet innovatsiyalari bo'yicha yetakchi sifatida AQSh kiberxavfsizlik, so'z erkinligi va raqamli savdoga e'tibor qaratib, dastlabki kiber-diplomatik tashabbuslarni shakllantirishda markaziy rol o'ynadi.

–Yevropa Ittifoqi: Yevropa Ittifoqi kiberxavfsizlik siyosatini uyg'unlashtirish va shaxs ma'lumotlarni himoya qilish va maxfiylik standartlarini himoya qilish bo'yicha strategiyalarni qabul qildi.

–Xitoy va Rossiya: Bu davlatlar kibermakonda davlat suverenitetiga e'tibor berishni ta'kidlab, internet boshqaruvining muqobil qarashlarini ilgari surdilar.

Kiber diplomatiyaning asosiy xususiyatlari quyidagilarda namoyon bo'ladi:

Kiber diplomatiya ko'p tomonlama hamkorlikni talab qiladi, bunda nomenklatura sifatida mamlakatlar umumiy normalar va asoslarni ishlab chiqish uchun birgalikda ishlashga majburlar.

1. Ko'p tomonlama manfaatdor tomonlar ishtiroki: an'anaviy diplomatiyadan farqli o'laroq, kiberdiplomatiya ko'pincha nodavlat ishtirokchilarni, jumladan, transmilliy korporatsiyalar, ilmiy doiralar va rivojlanayotgan fuqarolik jamiyatini o'z ichiga oladi.

2. Jadal rivojlanayotgan muhit: Texnologik innovatsiyalar sur'ati kiberdiplomatiya doimo yangi chaqiriqlarga moslashishi kerakligini ko'rsatdi.

3. Transchegaraviy tabiat: kiber muammolar milliy chegaralardan oshib ketdi va hamkorlikda xalqaro yondashuvlarni talab qilmoqda.

Samarali kiber diplomatiya texnologiya va uning oqibatlarini chuqur tushunishni talab qiladi. Diplomatlar kiberxavfsizlik va ma'lumotlarni himoya qilishning nozik tomonlarini o'rganish uchun texnik mutaxassislar bilan birga ishlash(kollaboratsiya)ni yo'lga qo'yishlari kerak. Chunki kiber diplomatiya muhim infratuzilmani himoya qilish va zararli dasturlar tarqalishining oldini olish kabi kibermakondagi xatti-harakatlar uchun global miqyosda qabul qilingan normalarni yaratishga qaratilgan.

Profilaktika va ta'sir choralari ham borki, ular kiberhujumlarning oldini olish choralari va tizimda buzilishlar sodir bo'lganda samarali javob berish mexanizmlarini o'z ichiga oladi.

Geosiyosiy nuqtai nazardan esa, kiberdiplomatiya milliy xavfsizlikni ta'minlash vositasi bo'lib xizmat qiladi. Mamlakatlar kiber tahdidlarning oldini olish va strategik manfaatlarini himoya qilish uchun diplomatik tashabbuslarni ilgari suradi.

Kiberdiplomatiyaning axloqiy jihatlari ham borki, u so'z erkinligi va shaxsiy daxlsizlikni himoya qilishni o'z ichiga oladi. Kiber ekspertiza bo'yicha global forum kabi tashabbuslar internetga to'g'ri maqsadda kirishni ta'minlash uchun internet etiketi hamda foydalanuvchilar salohiyati(axborot gigiyenasi)ni oshirish tarafdoridir.

Raqamli iqtisod kiberdiplomatiya uchun markaziy o'rinni egallaydi. Muzokaralar ko'pincha raqamli tijoratni ta'minlash, intellektual mulkni himoya qilish va innovatsiyalarni rag'batlantirishga qaratilgan.

Huquqiy bazalar ko'plab kiber diplomatik tashabbuslarga asoslanadi. Xalqaro huquq kiberoperatsiyalar uchun javobgarlikni joriy etish va kelishilgan me'yorlarga rioya etilishini ta'minlashda hal qiluvchi rol o'ynaydi.

Bugungi kunda kiber diplomatiyada qanday muammolar mavjud bo'lishi mumkin?

Atributning murakkabligi

–Kiber hodisalarning aybdorlarini aniqlash juda qiyin, bu davlatlar yoki aktorlarni javobgarlikka tortish harakatlarini murakkablashtiradi.

Universal me'yorlarning yo'qligi

–Turli xil milliy manfaatlar umume'tirof etilgan kiber me'yorlarning o'rnatilishiga to'sqinlik qilib, boshqaruvning parchalanishiga olib keldi.

Texnologik nomutanosibliklar

–Davlatlar o'rtasida texnologik imkoniyatlarning sezilarli nomutanosibligi kuch nomutanosibligini (muvozanatsizligi) keltirib chiqarishi mumkin. Bu esa jamoaviy harakatlar samaradorligini cheklaydi.

Kiberjinoyatlarning kuchayishi

–Kiberdiplomatiya tobora hukumatlar, xususiy tuzilmalar va huquqni muhofaza qilish idoralari o'rtasida yaqin hamkorlikni talab qiluvchi transmilliy kiberjinoyatchilikka qarshi kurashish muammosiga duch kelmoqda.

Milliy manfaatlarning qarama-qarshiligi

–AQShning ochiq internet modelidan Xitoyning markaziy boshqaruv yondashuvigacha bo'lgan kibermakonni boshqarishdagi turli qarashlarning mavjudligi – davlatlarni konsensusga erishtirish uchun jiddiy muammolarni keltirib chiqaradi.

Tezkor texnologik o'zgarishlar

–Innovatsiyalar ko‘lami ko‘pincha diplomatik tizimlarning moslashish qobiliyatidan oshib ketadi. Bu esa tartibga solish va ijro etishda bo‘shliqlarni keltirib chiqaradi.

Global boshqaruvning parchalanishi

–Kibermakonni boshqarish bo‘yicha umume'tirof etilgan tartibga soluvchi organning yo‘qligi tarqoq va ko‘pincha bahslarga sabab bo‘ladi.

Kiberdiplomatiyaning muhim bosqichlari

Kiberme'yorlarni o‘rnatish

Kibermakonda davlatning mas'uliyatli xulq-atvor normalarini ishlab chiqish sa'y-harakatlari kiberdiplomatiya uchun markaziy o‘rinni egalladi:

–*Tallin qo‘llanmasi (2013): Ushbu nashr xalqaro huquqning kiberoperatsiyalarga qanday tatbiq etilishi bo‘yicha yo‘l-yo‘riqni taqdim etadi.*

–*2015-yil BMT Hukumat ekspertlar guruhi hisobotida muhim infratuzilmani himoya qilish va zararli kiberfaoliyatning oldini olishning kabi asosiy tamoyillarni ko‘rsatib berdi.*

Mintaqaviy va ko‘p tomonlama asoslarni shakllantirish

–*Janubi-Sharqiy Osiyo davlatlari assotsiatsiyasi (ASEAN) kiberxavfsizlik tahdidlarini hamkorlikda hal qilish uchun mintaqaviy asoslarni ishlab chiqdi.*

–*NATO kibermakonni operatsiyalar o‘tkazish tarmog‘i sifatida ko‘rib, mudofaa strategiyalariga integratsiya qila oldi.*

XXI asrda kiber diplomatiya

Kiberhujumlarning roli

Yirik kiber hodisalar kiberdiplomatiya trayektoriyasini shakllantirib, tizimdagi zaifliklarni yuzaga chiqardi va xalqaro choralar ko‘rishga chaqirdi. Kiberhujumlarning ko‘pchiligi oddiy ko‘rinishda bo‘lsa-da, ba’zida ularning ko‘lami va keltirib chiqargan zarari e’tiborni tortadi. So‘nggi o‘n yillikdagi eng mashhur kiberhujumlarni ko‘rib chiqamiz:

WannaCry: Haqiqiy epidemiyaga aylangan hujum

WannaCry hujumi butun dunyo bo‘ylab ransomware va kiber zararli dasturlarni tanitgan yirik voqea hisoblanadi. Shadow Brokers tomonidan ommaga oshkor qilingan Equation Group ekspluatlarini qo‘llagan holda yaratilgan ushbu ransomware tarmoq orqali tez tarqalish qobiliyatiga ega edi. Xususan, 4 kun davomida WannaCry 150 mamlakatda 200,000 dan ortiq kompyuterlarni ishdan chiqardi. Shu qatorda shifoxonalar, ishlab chiqarish korxonalari va boshqa muhim infratuzilmalar ham zarar ko‘rdi. WannaCry hali ham faol va jahon kompyuterlariga tahdid solib kelmoqda.

NotPetya/ExPetr: Eng katta zarar keltirgan kiberhujum

NotPetya hujumi WannaCry kabi ransomware bo‘lsa-da, u aslida "wiper" edi, ya'ni fayllarni qayta tiklab bo‘lmaydigan darajada o‘chirish uchun yaratilgan edi. Bu hujumning

asosiy nishoni biznesmenlar edi, ayniqsa moliyaviy dastur MeDoc orqali tarqalgan. Ushbu hujum \$10 milliard miqdorida zarar keltirdi va hujum global bizneslar uchun jiddiy iqtisodiy yo'qotishlarga olib keldi. (WannaCry esa \$4–8 milliard atrofida baholangan).

Stuxnet: Kiberqurolning ilk namoyishi

Stuxnet dunyodagi eng murakkab va mashhur zararli dasturlardan biri bo'lib, Eronning uran boyitish sentrifugalarini buzish orqali mamlakatning yadroviy dasturini bir necha yilga orqaga surdi. Internet yoki mahalliy tarmoqqa ulanmagan kompyuterlarga USB flesh-disklar orqali kirib, Siemens boshqaruv kontrollerlari yordamida uran boyitish jarayonini buzgan. Bu zararli dastur xalqaro miqyosda sanoat tizimlariga qarshi kiber qurollarning samaradorligini namoyish etdi.

DarkHotel: Mehmonxonadagi josuslik

DarkHotel hujumi orqali yuqori lavozimli rahbarlar va nufuzli shaxslarning qurilmalari mehmonxona tarmoqlaridan foydalangan holda, josuslik dasturi bilan zararlangan. Huquqbuzarlar soxta dasturiy ta'minot yangilanishlarini taqdim qilib, qurilmalarni infeksiyalashgan. Ushbu zararli dastur klaviatura kiritmalarini kuzatgan va nishonli hujumlarini amalga oshirish imkoniyatini bergan

Mirai: Internet qulashiga olib kelgan botnet

IoT (Internet of things) qurilmalarining ommaviy ravishda himoyasizligi Mirai botnetining yaratilishiga olib keldi. Ushbu botnet millionlab raqamli qurilmalarni birlashtirib, 2016-yil 21-oktabrda DNS provayder Dyn-ga qarshi ulkan DDoS hujum uyushtirgan. Natijada PayPal, Twitter, Netflix kabi xizmatlar vaqtincha ishlamay qoldi. IoT xavfsizligini kuchaytirish zarurligi yana bir bor isbotlandi.

Kiberhujumlardan himoya qilish zamonaviy dunyoda davlatlar, tashkilotlar va jismoniy shaxslar uchun hayotiy ahamiyatga ega. Quyida uning asosiy sabablari keltirilgan:

–Kiberhujumlar natijasida shaxsiy, moliyaviy yoki maxfiy ma'lumotlar o'g'irlanishi mumkin. Mudofaa choralarining samarali bo'lishi ushbu ma'lumotlarni himoya qilishni ta'minlaydi.

–Kiberhujumlar korxonalar va davlatlar uchun katta moliyaviy zarar keltirishi mumkin. Himoya choralari esa moliyaviy barqarorlikni ta'minlaydi.

–Mijozlar va fuqarolar xavfsizlik choralariga ishonishlari uchun kiberhimoya choralari muhimdir. Bu jamoaviy imidj va davlat barqarorligiga hissa qo'shadi.

–Hujumlar muhim infratuzilma tizimlariga (masalan, energiya, transport, sog'liqni saqlash) zarar yetkazishi mumkin. Himoya choralari bu tizimlarning uzluksiz ishlashini ta'minlaydi.

–Davlatlar o'rtasidagi kiberhujumlar siyosiy nizolarga olib kelishi mumkin. Mudofaa choralarining kuchaytirilishi xalqaro munosabatlarda barqarorlikni saqlashga yordam beradi.

Kiberhimoyaga e'tibor berish bugungi raqamli dunyoda rivojlanish va barqarorlikning ajralmas qismidir. Bu sohada texnologiyalarni rivojlantirish va xodimlarni o'qitish muhim ahamiyatga ega. An'anaviy diplomatiyadan farqli o'laroq, kiberdiplomatiya turli aktorlarni, jumladan texnologik kompaniyalar, nodavlat tashkilotlari va akademik doiralarni o'z ichiga oladi. Kibermakon barqarorligi bo'yicha global komissiya (GCSC) kabi tashabbuslar o'ziga xos yondashuvni aks ettiradi.

Kiberdiplomatiyaning kelajakdagi istiqbollari:

Kiberdiplomatiya tarixi shuni ko'rsatadiki, uning kelajagi texnologik innovatsiyalar, geosiyosiy dinamika va global hamkorlikning o'zaro ta'sirida shakllanadi. Asosiy tendensiyalarga quyidagilar kiradi:

–Majburiy kelishuvlarni ishlab chiqish: Kibermakonni boshqarish bo'yicha yuridik jihatdan majburiy shartnomalarni yaratish bo'yicha sa'y-harakatlarini kuchayishi kerak.

–Sun'iy intellekt va kiber diplomatiya jipslashuvi: sun'iy intellektga asoslangan vositalar kiber hodisalarni boshqarish va muzokaralarni osonlashtirishda muhim rol o'ynaydi.

–Mintaqaviy hamkorlikni kuchaytirish: Mintaqaviy tashkilotlar mahalliyashtirilgan kibertahdidlarga qarshi kurashda yetakchilikni davom ettirishlari lozim bo'ladi.

–Xalqaro hamkorlikni mustahkamlash: Kiberdiplomatiya davlatlarga kiberterrorizm va sun'iy intellektdan noto'g'ri foydalanish kabi global muammolarda hamkorlik qilish uchun platforma yaratadi.

–Innovatsiya va rivojlanishni rag'batlantirish: Hamkorlik kelishuvlari orqali mamlakatlar innovatsiyalarni rivojlantirishi va raqamli resurslardan adolatli foydalanishni ta'minlashi mumkin.

–Imkoniyatlarni oshirish: Kiberdiplomatiya rivojlanayotgan mamlakatlarga kiberxavfsizlik infratuzilmasi va tajribasini oshirishga yordam berish uchun salohiyatni oshirish tashabbuslarini ilgari surishi mumkin.

–Kiber diplomatiyaning kelajagi: Kibermakon globallashtirish uchun tobora ajralmas bo'lib borar ekan, kiber diplomatiyaning ahamiyati o'sishda davom etadi.

–Kibermakondagi xatti-harakatlar bo'yicha majburiy xalqaro shartnomalar ishlab chiqishning ortishi mumkin.

–Kiber diplomatiyada sun'iy intellekt: kiber tahdidlarni bashorat qilish, oldini olish va ularga samarali javob berish uchun sun'iy intellekt vositalaridan foydalanish mumkin.

–Kengaytirilgan davlat-xususiy sheriklik: kibermakonni himoya qilish uchun hukumatlar va xususiy texnologiya kompaniyalari o'rtasida chuqurroq hamkorlik olib borish lozim.

–Mintaqaviy tashabbuslar: Yevropa Ittifoqining kiberxavfsizlik strategiyasi kabi mintaqaviy hamkorlikka ko‘proq e‘tibor qaratish kerak.

–Sun‘iy intellektning kiberoperatsiyalarga integratsiyalashuvi avtomatlashtirilgan hujumlar va kuchayish xavfini oshirdi.

–Deepfake texnologiyasi: sun‘iy intellekt tomonidan yaratilgan deepfakes borgan sari dezinformatsion kampaniyalarda qo‘llanilib, ishonchga putur yetkazadi va jamiyatlarni beqarorlashtiradi.

–Avtonom kiber qurollar: kiberhujumlarda sun‘iy intellektga asoslangan vositalardan foydalanish kutilmagan oqibatlariga olib kelishi va inson nazoratini yo‘qotishi haqida xavotir uyg‘otadi.

–Kvant hisoblashdagi yutuqlar joriy shifrlash usullarini ehtimoliy ravishda eskirib, xavfsiz aloqa va ma‘lumotlarni himoya qilishda zaifliklarni keltirib chiqarishi mumkin.

–Noto‘g‘ri ma‘lumotlar va axborot urushi: dezinformatsion kampaniyalar jamoatchilik fikriga ta‘sir qilish va demokratik jarayonlarni beqarorlashtirish uchun kuchayib borayotgan unsurdir.

–Saylovga aralashuv: Kiberdiplomatiya dezinformatsiya va hakkerlik orqali saylovlarni manipulyatsiya qilish bo‘yicha transchegaraviy sa‘y-harakatlarni hal qilishi kerak.

–Ijtimoiy media manipulyatsiyasi: platformalardan zararli kontentni tarqatish orqali jamiyat birligini buzish uchun tobora ko‘proq foydalanilmoqda.

–Tartibga solish platformalarining muammolari: Texnologik kompaniyalar ko‘pincha chegaralar orqali ishlaydi. Bu kontentni tartibga solish va me‘yorlarni qo‘llash bo‘yicha harakatlarni murakkablashtiradi. So‘z erkinligini zararli kontentni cheklash zarurati bilan malakalash kiberdiplomatiyada bahsli masala bo‘lib qolmoqda.

–Ochiq internet tarafdorlari va davlat tomonidan boshqariladigan modellar tarafdorlari o‘rtasida davom etayotgan bahs-munozaralar kuchayib bormoqda. AQSh modeli bepul, ochiq va o‘zaro hamkorlikda asoslangan internet tarafdori bo‘lsa, Xitoy va Rossiya modeliga ko‘ra “kiber suverenitet”ni rag‘batlantiradi.

–Internetning parchalanishi. Mamlakatlar alohida raqamli ekotizimlarni yaratadigan "parchalangan internet" tendensiyasi global hamkorlik uchun muammolarni keltirib chiqaradi. Ushbu parchalanish transchegaraviy ma‘lumotlar oqimiga to‘sqinlik qilishi va internetning global tabiatiga putur yetkazishi mumkin.

– Kosmosni tadqiq etishga asoslangan kiber operatsiyalar: aloqa uchun sun‘iy yo‘ldosh tizimlariga tobora ortib borayotgan bog‘liqlik kosmik kiber operatsiyalarda zaifliklarni keltirib chiqaradi.

–Sun’iy intellekt va ma’lumotlardan foydalanishning axloqiy muammolari: sun’iy intellektning axloqiy oqibatlari, ayniqsa kuzatuv va ma’lumotlarni yig’ishda kiber diplomatiya uchun uzoq muddatli muammolarni keltirib chiqaradi. Innovatsiyalarni shaxsiy hayot va inson huquqlari bilan muvozanatlash juda muhimdir.

–Kiberinfratuzilmaning global atrof-muhitga ta’siri: Ma’lumotlar markazlari va raqamli tarmoqlar kengayib borar ekan, ularning ekologik oqibati dolzarb muammoga aylanadi. Kiberdiplomatiya raqamli rivojlanishni muhokama qilishda barqarorlikni hisobga olishi kerak.

–Barqaror xalqaro qoidalar yaratilishi: BMT va boshqa xalqaro tashkilotlarning hamkorlikda ishlab chiqqan kibermakon qoidalari davlatlararo ziddiyatlarni kamaytirishi kutilmoqda.

–Texnologik taraqqiyot va xavfsizlik muvozanati: Sun’iy intellekt va blokcheyn texnologiyalarining jadal rivojlanishi xavfsizlikni ta’minlashda yangi imkoniyatlar yaratadi.

–Xususiy sektor va davlat hamkorligi: Kibermakondagi muammolarni hal qilish uchun davlat va xususiy sektor o’rtasidagi hamkorlik yanada kengayadi.

–Ta’lim va malaka oshirish: Xalqaro statistikaga ko’ra, 2030-yilga kelib, kiberxavfsizlik sohasida malakali kadrlar ehtiyoji 50% ga oshishi bashorat qilinmoqda.

Xulosa:

Raqamli texnologiyalarning jadal rivojlanishi global sahnaga misli ko’rilmagan imkoniyatlar va muammolarni keltirib chiqardi. Kiberdiplomatiya, xalqaro munosabatlarni boshqarish va kibermakondagi muammolarni hal qilish sohasi hozir har qachongidan ham muhimroq. Biroq, raqamli sohaning murakkabligi, jadal rivojlanishi va turli manfaatdor tomonlar innovatsion yondashuvlarni talab qiladigan o’ziga xos muammolarni keltirib chiqaradi.

Kiberdiplomatiyaning kelib chiqishi texnologik taraqqiyot bilan birga diplomatiya evolyutsiyasining ham keng tarixini aks ettiradi. Kiberdiplomatiya o’zining dastlabki internet davridagi ildizlaridan tortib toki xalqaro munosabatlarda muhim soha sifatida paydo bo’lgunigacha nafaqat raqamli davrning qiyinchiliklari balki imkoniyatlarini ham o’zida mujassam etadi.

Uning tarixini tushunish kibermakonning murakkabliklarini tartibga solish va doimiy o’zgarib turadigan sohada tinchlik, hamkorlik va xavfsizlik tamoyillari ustunligini ta’minlash uchun juda muhimdir.

Kiberdiplomatiya nafaqat tahdidlarni bartaraf etish, balki xalqaro barqarorlikni ta’minlash uchun muhim mexanizm hisoblanadi. Davlatlar, tashkilotlar va xususiy sektor o’rtasidagi hamkorlikni kuchaytirish orqali kibermakondagi nizolarni kamaytirish, texnologik taraqqiyot imkoniyatlaridan samarali foydalanish va umumiy barqarorlikni ta’minlash mumkin. Bu yo’nalishda ilmiy tadqiqotlar, xalqaro tajriba almashinuvi va huquqiy me’yorlarning rivojlanishi

ustuvor vazifa bo'lib qoladi. Ushbu muammolarni hal qilish uchun kiber diplomatiya ko'p tomonlama hamkorlikka, turli manfaatdor tomonlarni qamrab olishga va moslashuvchan, istiqbolli asoslarni ishlab chiqishga ustuvor ahamiyat berishi kerak. Kiberdiplomatiya xalqaro munosabatlardagi o'zgaruvchan chegarani ifodalaydi. Bu texnik innovatsiyalar geosiyosiy strategiya, axloqiy mulohazalar va global hamkorlikka javob beradigan sohadir. Atribut va normalarning parchalanishi kabi muammolar saqlanib qolsa-da, kibermakonda tinchlik, xavfsizlik va farovonlikni mustahkamlash imkoniyatlari juda katta.

Davlatlar, tashkilotlar va shaxslar raqamli asrning murakkabliklarida harakat qilishda davom etar ekan, kiber diplomatiya hamma uchun xavfsiz, o'ziga xos va mustahkam kibermakonni yaratishga qaratilgan sa'y-harakatlarning asosi bo'lib qoladi.

Foydalanilgan adabiyotlar:

1. UN official web site: <https://www.un.orgofficial>
2. Soft Power. Joseph S. Nye, Jr. Foreign Policy, No. 80, Twentieth Anniversary (Autumn, 1990), pp. 153-171
3. Cyber Power. Joseph S. Nye, Jr. Copyright 2010 President and Fellows of Harvard College, pp. 9-16
4. <https://www.sciencedirect.com/science/article/pii/S1877050920318317>
5. <https://www.sciencedirect.com/science/article/pii/S026736492400075X>
6. <https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/>
7. <https://cybersecurityventures.com/>
8. https://www.researchgate.net/publication/366516762_Cyber_Diplomacy_under_Increased_Competition_Between_the_Great_Powers