KIBER MAKONDA QUROLLI MOJAROLAR: XALQARO GUMANITAR HUQUQNING YANGI SINOVLARI VA QO‘LLANILISH CHEGARALARI

Maxmatqulova Saida Ilxom qizi
Toshkent davlat yuridik universiteti magistranti.

https://doi.org/10.5281/zenodo.16627540

Annotatsiya. *Mazkur maqolada kiber makonda yuzaga kelayotgan qurolli mojarolar doirasida xalqaro gumanitar huquq (XGH) me’yorlarining tatbiq etilishi, ularning huquqiy va amaliy muammolari tahlil qilinadi. Raqamli texnologiyalarning harbiy maqsadlarda tobora faol qo‘llanilishi XGH tamoyillarining – ajratish, proporsionallik va ehtiyot choralarini ko‘rish prinsiplari – zamonaviy kiber harakatlarga qanday moslashishini qayta ko‘rib chiqishni taqozo qilmoqda. Tadqiqot davomida xalqaro huquqshunoslikdagi eng nufuzli yondashuvlar, xususan Tallin qo‘llanmasi asosida XGHning amaldagi zaif jihatlari ko‘rsatilib, mavjud normativ bo‘shliqlar aniqlanadi. Shu bilan birga, ayrim davlatlarning milliy strategiyalari tahlili orqali xalqaro huquqning zamonaviy urush shakllariga ta'siri va yetishmovchiligi yoritiladi. Muallif kiber makonda inson huquqlari va xalqaro tinchlikni ta’minlashda XGHning moslashtirilgan va kuchaytirilgan huquqiy mexanizmlar bilan boyitilishi lozimligini asoslaydi.*

Kalit so‘zlar: *xalqaro gumanitar huquq, kiber mojaro, qurolli mojaro, proporsionallik prinsipi, ajratish prinsipi, ehtiyot chorasi, Tallin qo‘llanmasi, xalqaro huquq, raqamli xavfsizlik, kiber urush, xalqaro nizolar.*

Kiber makonda qurolli mojarolar va ularga xalqaro gumanitar huquqning (bundan keyin matnda XGH) qo‘llanishi masalasi XXI asr global xavfsizligi, texnologik taraqqiyot va xalqaro huquqning moslashuvchanligiga oid eng dolzarb yo‘nalishlardan biridir. An'anaviy qurolli mojarolar fazosi endilikda faqat quruqlik, havo, suv va kosmik makon bilan cheklanmay, balki raqamli maydonni ham o‘z ichiga olmoqda. Kiber makon – bu faqat aloqa, axborot va ma'lumotlarni uzatish tizimi emas, balki davlatlar o‘rtasidagi qarama-qarshiliklar, hujum va himoya strategiyalari tobora faol rivojlanayotgan urush maydonidir. Shu nuqtai nazardan, xalqaro gumanitar huquqning mazkur zamonaviy sohadagi qo‘llanilish imkoniyatlarini, u duch kelayotgan sinovlar va cheklovlarni tahlil qilish zarurati yuzaga chiqmoqda.

Xalqaro gumanitar huquq qurolli mojarolar vaqtida insoniyat azobini kamaytirishga, fuqarolik aholisi va harbiy bo‘lmagan obyektlarni himoya qilishga qaratilgan qoidalar majmuidir. Ushbu huquqiy rejim asosan 1949-yilgi to‘rtta Jeneva konvensiyasi [1] va ularning 1977 va 2005-yilgi qo‘shimcha protokollarida mustahkamlangan. Biroq bu huquqiy asoslar XX asr urushlarining kontekstida ishlab chiqilgan bo‘lib, ularning kiber makondagi zamonaviy qurolli mojarolarga qay darajada tatbiq etilishi hali-hanuz xalqaro huquqshunoslik doirasida bahsli va izlanishga ochiq masala bo‘lib qolmoqda.

XXI asrda texnologik taraqqiyotning tez sur’atlari va raqamli texnologiyalarning keng tarqalishi urush tabiatini tubdan o‘zgartirdi. An’anaviy harbiy operatsiyalar bilan bir qatorda, kiber makon qurolli mojarolarning yangi maydoniga aylandi. Kiber hujumlar endilikda davlatlarning xavfsizlik strategiyalarining ajralmas qismiga aylanib, XGH zamonaviy yo‘nalishlarini shakllantirishda hal qiluvchi o‘rin tutmoqda.

Kiber qurolli mojarolarni XGH doirasida tartibga solishning birinchi va eng muhim bosqichi ularning huquqiy tabiatini to‘g‘ri aniqlashdan iborat. Xalqaro Qizil Xoch Qo‘mitasining ta’kidlashicha, kiber operatsiyalar qurolli mojaro kontekstida amalga oshirilganida, ularga XGH me’yorlari to‘liq tarzda qo‘llaniladi [2]. Biroq, amalda kiber hujumni qurolli kuch ishlatish

sifatida tasniflovchi aniq mezonlarni belgilash murakkabroq masala hisoblanadi.

Tallinn Manual loyihasi doirasida amalga oshirilgan tadqiqotlar shuni ko‘rsatadiki, kiber hujumni qurolli hujum sifatida tasniflovchi asosiy mezonlar quyidagilardan iborat: birinchidan, jismoniy obyektlarga zarar yetkazish yoki ularni yo‘q qilish imkoniyati, ikkinchidan, hujumning oqibatlari an’anaviy qurolli hujumning natijalariga o‘xshash bo‘lishi, uchinchidan, hujumning bevosita ta’siri natijasida inson o‘limi yoki jiddiy jarohatlar yuzaga kelishi.

Biroq, bu mezonlarni amalda qo‘llash sezilarli qiyinchiliklarga duch keladi. Masalan, 2010-yilda Eron yaderli dasturiga qarshi amalga oshirilgan Stuxnet virusi harbiy obyektga qarshi yo‘naltirilgan bo‘lsa-da, uning ta’siri texnik tizimlarning buzilishi bilan cheklandi [3]. Bunday holatda kiber hujumni qurolli hujum sifatida tasniflovchi aniq huquqiy asoslar mavjud emas.

Shuningdek, kiber hujumlarning xarakteristik xususiyatlaridan biri ularning ko‘p bosqichli va uzoq muddatli ta’siriga ega bo‘lishidir. Kiber hujum natijasida sodir bo‘lgan zarar darhol namoyon bo‘lmasligi va vaqt o‘tishi bilan kuchayib borishi mumkin [4]. Bu esa hujumning qurolli xarakterini aniqlashda qo‘shimcha murakkabroq masalalar tug‘diradi.

Kiber makonning xalqaro huquq doirasida tartibga solinishi 2000-yillardan boshlab intensiv tus oldi. BMT Bosh Assambleyasi doirasida Axborot xavfsizligi bo‘yicha hukumatlararo ekspertlar guruhi (GGE) tomonidan bir necha rezolyutsiyalar va hisobotlar ishlab chiqildi. Xususan, 2013 va 2015-yillardagi hisobotlarda davlatlarning kiber fazodagi xatti-harakatlari ham xalqaro huquqqa, shu jumladan XGHga muvofiq bo‘lishi lozimligi alohida qayd etilgan [5]. Bu yondashuv BMT nizomining 2(4)-moddasidagi kuch ishlatmaslik tamoyili va 51-moddasidagi [6] o‘zini himoya qilish huquqi bilan hamohangdir.

Qurolli mojaroning mavjudligini aniqlash XGHning qo‘llanilishi uchun muhim shartdir. Kiber hujumlar esa ko‘plab hollarda bevosita jismoniy zarar yetkazmaydi yoki an'anaviy qurolli harakatlar kabi aniqlik kasb etmaydi. Shu bois, kiber hujumlar doirasida mojaroning “xalqaro” yoki “xalqaro bo‘lmagan” xususiyatini aniqlash o‘ta murakkabdir. Masalan, Estoniyaga 2007-yilda qilingan DDoS hujumlar natijasida davlatning bank tizimi, ommaviy axborot vositalari va hukumat saytlariga ulanish butunlay to‘xtagan bo‘lsa-da, ushbu holat xalqaro qurolli mojaro sifatida baholanmagan [7].

XGHning asosiy prinsipi – ajratish (distinction) – harbiy va fuqarolik obyektlari o‘rtasidagi farqni saqlashni talab qiladi. Ammo kiber makonda bu chiziq ko‘pincha noaniq bo‘ladi. Masalan, davlat hokimiyatiga tegishli serverlarda fuqarolar ma’lumotlari ham saqlanishi mumkin, bu esa ularni harbiy obyekt sifatida nishonga olishni XGH doirasida murakkablashtiradi. Shu jihatdan, ajratish prinsipi kiber fazoda an’anaviy urushlardagidek aniq va samarali qo‘llanilmasligi ayon bo‘lmoqda [8].

ICRC tomonidan ishlab chiqilgan ko‘rsatmalarga ko‘ra, kiber hujum amalga oshiruvchilar hujum obyektining harbiy yoki fuqarolik tabiatini aniq aniqlash majburiyatiga ega [9]. Biroq, kiber makonda obyektlarning funktsional tasnifi dinamik xarakterga ega bo‘lib, bir obyekt turli vaqtlarda turli maqsadlarda ishlatilishi mumkin.

Bundan tashqari, kiber hujumlar ko‘pincha tarmoq orqali tarqaladi va dastlabki maqsaddan tashqari obyektlarga ham ta’sir ko‘rsatishi mumkin [10]. Bu esa hujum amalga oshiruvchilardan oldindan barcha mumkin bo‘lgan oqibatlarni hisobga olishni talab qiladi, ammo amalda bu doimo amalga oshirilishi mumkin emas.

XGHdagi yana bir muhim prinsip – proporsionallik (proportionality) prinsipidir. Unga ko‘ra, hujumda erishiladigan harbiy ustunlik fuqarolik aholiga yetadigan zarar bilan solishtirilib, muvofiq bo‘lishi kerak. Kiber hujumlarda bu muvofiqlikni baholash juda murakkab, chunki

hujum oqibatlari zudlik bilan aniqlanmasligi, zanjirli tarzda tarqalishi yoki kutilmagan oqibatlarga olib kelishi mumkin. Shu sababli kiber hujumlar XGHning proporsionallik prinsipiga ziddilik tug‘dirishi mumkin.

Kiber hujumlarning ta’siri ko‘pincha kaskad effekti ko‘rinishida namoyon bo‘ladi, ya’ni bitta tizimning buzilishi bir qancha boshqa tizimlarga ham ta’sir ko‘rsatadi [11]. Masalan, ma’lum bir harbiy obyektga qarshi yo‘naltirilgan kiber hujum elektr tarmoqlariga ta’sir ko‘rsatishi va natijada kasalxonalar, maktablar hamda boshqa fuqarolik muassasalarining faoliyatini to‘xtatishi mumkin.

Shuningdek, kiber hujumlarning harbiy samaradorligini baholash ham aniq mezonlarga ega emas. An’anaviy harbiy operatsiyalardan farqli o‘laroq, kiber hujumlar bevosita jismoniy yo‘q qilishga olib kelmasdan, raqobatchining hatti-harakatlarini cheklash yoki ma’lumotlarni o‘g‘irlash maqsadlarini ko‘zlashi mumkin.

Ehtiyot choralarini ko‘rish prinsipi (precaution) ham kiber makonda qo‘llashda amaliy muammolarga duch keladi. Masalan, kiber hujum boshlanishidan oldin uning texnik va ijtimoiy oqibatlarini to‘liq bashorat qilish deyarli imkonsizdir. Bu esa ehtiyot choralarini yetarli darajada ko‘rish imkonini cheklaydi [12]. Kiber makonda ushbu majburiyatlarni bajarish texnik va huquqiy jihatdan murakkab masala hisoblanadi.

Birinchidan, kiber hujumlarning aniqligini ta’minlash zamonaviy texnologiyalar bilan ham to‘liq kafolatlanmaydi. Zararli dastur yoki kiber qurol aniq maqsadga qaratilgan bo‘lsa ham, u tarmoq orqali tarqalishi va kutilmagan obyektlarga ham ta’sir ko‘rsatishi mumkin [13]. Bu holda hujum amalga oshiruvchilar dastlabki rejadan chetga chiqishni oldini olish uchun qo‘shimcha texnik choralar ko‘rishga majbur bo‘ladi.

Ikkinchidan, kiber hujumlarning vaqt jihatidan cheklanganligini ta’minlash ham muammoli masala hisoblanadi. Zararli dasturlar kompyuter tizimlariga kirib borganidan so‘ng, ularni to‘liq nazorat qilish va kerak vaqtda to‘xtatish har doim ham mumkin bo‘lavermaydi [14]. Bu esa XGH talablariga ko‘ra hujumning davomiyligini cheklash majburiyatini bajarishda qiyinchiliklar tug‘diradi.

Uchinchidan, kiber hujumlar natijasida yuzaga kelgan zararni tiklash masalasi ham alohida e’tibor talab qiladi. An’anaviy urush sharoitida buzilgan infratuzilmani tiklash nisbatan aniq jarayonlarni talab qiladi, ammo kiber hujumlar natijasida buzilgan axborot tizimlari va ma’lumotlarni tiklash murakkabroq va uzoq muddatli jarayon.

Kiber qurolli mojarolarning o‘ziga xos jihati shundaki, ular nafaqat jismoniy obyektlarga balki ma’lumotlarga ham ta’sir ko‘rsatishi mumkin. Fuqarolik ma’lumotlarini himoya qilish masalasi XGH doirasida nisbatan yangi yo‘nalish bo‘lib, zamonaviy kiber hujumlar kontekstida alohida ahamiyat kasb etadi [15].

Shaxsiy ma’lumotlar, tibbiy kartalar, moliyaviy ma’lumotlar kabi fuqarolik ma’lumotlari kiber hujumlar vaqtida bevosita nishon bo‘lishi yoki tasodifiy ravishda zarar ko‘rishi mumkin. XGH me’yorlari bo‘yicha bunday ma’lumotlarni himoya qilish majburiyati mavjud, ammo kiber makonda bu majburiyatni qanday amalga oshirish masalasi aniq tartibga solinmagan.

ICRC ning pozitsiyasiga ko‘ra, fuqarolik ma’lumotlariga qarshi yo‘naltirilgan kiber hujumlar XGH buzilishi hisoblanadi va bunday hujumlardan qochish majburiyati mavjud [16]. Biroq, harbiy obyektlarga qarshi amalga oshirilayotgan kiber hujumlar davomida fuqarolik ma’lumotlarini himoya qilish uchun qanday texnik choralar ko‘rish kerakligi aniq belgilanmagan.

Shuningdek, ma’lumotlarning harbiy yoki fuqarolik tabiatini aniqlash ham murakkab

masala hisoblanadi. Ayrim ma'lumotlar ikki tomonlama maqsadlarda ishlatilishi mumkin va ularning aniq tasnifi kontekstga bog'liq bo'ladi.

Bunday murakkabliklar fonida XGHning kiber urushlar doirasida qanday ishlashini tushuntiruvchi yo'nalishlar ham mavjud. Shular jumlasidan Tallin qo'llanmasi (Tallinn Manual 1.0 va 2.0) kiber fazodagi harakatlarga xalqaro huquqning tatbiq etilishi yuzasidan eng nufuzli manba hisoblanadi. Bu qo'llanma NATOga a'zo davlatlarning ekspertlari tomonidan ishlab chiqilgan bo'lib, unda XGH tamoyillarining kiber fazodagi qo'llanilishi yuzasidan batafsil yondashuvlar keltirilgan. Masalan, Tallin qo'llanmasi 2.0da aytilishicha, agar kiber hujumlar jismoniy zarar, o'lim yoki muhim infrastrukturalarning ishdan chiqishiga olib kelsa, ular qurolli mojaro sifatida baholanishi mumkin [17].

Shunga qaramay, ushbu qo'llanma majburiy emas, balki tavsiyaviy xarakterga ega bo'lib, unda keltirilgan yondashuvlar ham xalqaro huquqshunoslar va davlatlar tomonidan bir xilda tan olinmagan. Bu esa XGHni kiber makonda qo'llash borasida yagona standartlarning yo'qligini ko'rsatadi.

Neytrallik prinsipi mojarodagi taraflarga qo'shilmagan davlatlarning hududlaridan harbiy maqsadlarda foydalanishni taqiqlaydi. Kiber makonda ushbu prinsipni qo'llash global internetning o'zaro bog'langan tabiati tufayli qiyinchiliklar tug'diradi.

Kiber hujumlar ko'pincha bir nechta davlatlar hududidagi serverlar va tarmoqlar orqali amalga oshiriladi. Bunday holatlarda tranzit davlatlarning neytrallik maqomini saqlash va ularning infratuzilmasidan harbiy maqsadlarda ruxsatsiz foydalanishga yo'l qo'ymaslik majburiyati paydo bo'ladi.

Biroq, kiber hujumlarning texnik xususiyatlari tufayli tranzit davlatlar ko'pincha o'z hududlaridan harbiy maqsadlarda foydalanilayotganidan xabardor bo'lmaydi. Bu holda neytrallik prinsipini buzish faktini aniqlash va javobgarlikni belgilash masalasi murakkablashadi.

Tallinn Manual ekspertlari tomonidan ta'kidlanganidek, neytral davlatlar o'z hududlaridan kiber hujumlar amalga oshirilishini oldini olish uchun yetarli choralar ko'rishi shart. Ammo, yetarli choralar tushunchasi kiber makon uchun aniq belgilanmagan va har bir holat alohida tahlil qilinishini talab qiladi.

Amaliy jihatdan, ba'zi davlatlar kiber fazodagi harakatlar uchun o'z milliy doktrinalarini ishlab chiqqan. AQShning 2018-yilgi Cyber Strategy hujjatida davlat kiber hujumlarga nisbatan harbiy javob berish huquqini saqlab qolganini e'lon qilgan [18]. Bu yondashuv esa kiber fazoda qurolli mojaro boshlanishi ehtimolini oshiradi va XGH qoidalarining qo'llanish zaruratini kuchaytiradi.

So'nggi yillarda sodir bo'lgan yirik kiber hujumlar XGH me'yorlarining amalda qo'llanilishi bo'yicha muhim tajriba to'plash imkonini berdi. 2007-yilda Estoniyaga qarshi amalga oshirilgan kiber hujumlar davlat infratuzilmasiga ta'sirining keng ko'lami va davomiyligi jihatidan yangi pretsident yaratdi [19].

2010-yildagi Stuxnet virusining Eron yaderli dasturiga ta'siri kiber qurolli mojarolarning texnik murakkabligi va noaniq oqibatlarini ko'rsatdi [20]. Ushbu hujum aniq harbiy maqsadga qaratilgan bo'lsa-da, uning tarqalishi va boshqa tizimlarga ta'siri dastlabki rejalardan tashqariga chiqdi.

2015-yilda Ukraina elektr tarmoqlariga qarshi amalga oshirilgan kiber hujumlar fuqarolik infratuzilmasiga ta'sirining keng ko'lami va insoniy oqibatlarini ko'rsatdi. Minglab odamlar elektr energiyasiz qoldi va bu holat XGH buzilishi sifatida baholandi.

Ushbu misollar shuni ko'rsatadiki, kiber hujumlar XGH me'yorlarini buzishi mumkin va

bunday buzilishlarni oldini olish uchun profilaktik choralar zarur. Shuningdek, kiber hujumlar natijasida yuzaga kelgan zararlarni baholash va javobgarlikni belgilash uchun yangi huquqiy mexanizmlar ishlab chiqish zarurati mavjud [21].

Kiber makonda qurolli mojarolarning rivojlanishi xalqaro gumanitar huquq uchun sezilarli yangi sinovlar tug‘dirmoqda. Mavjud XGH me’yorlari, umuman olganda, kiber operatsiyalarga qo‘llanilishi mumkin, ammo ularning amaliy tatbiqi bir qator murakkab masalalarni keltirib chiqaradi.

Eng muhim muammolardan biri kiber hujumlarning qurolli hujum maqomiga ega ekanligini aniqlash mezonlarining noaniqligidir. Jismoniy zarar yetkazish mezoni har doim ham kiber hujumlarning harbiy ahamiyatini to‘liq aks ettirmaydi, chunki zamonaviy urushda axborot ustunligi va tizimlarni buzish ham muhim rol o‘ynaydi.

Farqlash, proporsionallik va ehtiyotkorlik kabi asosiy XGH tamoyillarini kiber makonda qo‘llash texnik murakkablik tufayli qiyinchiliklar tug‘diradi. Kiber infratuzilmaning o‘zaro bog‘liqligi va ikki tomonlama maqsadlarda ishlatilishi bu tamoyillarni amalda realizatsiya qilishni murakkablashtiradi.

Fuqarolik ma’lumotlarini himoya qilish va neytrallik prinsipini saqlash masalalari kiber makonda yangi huquqiy yo‘nalishlar sifatida shakllanmoqda va qo‘shimcha tartibga solishni talab qiladi. Mavjud xalqaro huquqiy base ushbu masalalarni to‘liq qamrab olish uchun rivojlantirilishi zarur.

Kiber qurolli mojarolarni tartibga solishda Tallinn Manual kabi akademik loyihalar muhim hissa qo‘shmoqda, ammo ular majburiy kuchga ega emas. Kelajakda kiber makondagi qurolli mojarolarni aniq tartibga soluvchi xalqaro shartnomalar ishlab chiqish zarurati mavjud.

Shu bilan birga, kiber hujumlar bo‘yicha dalillar to‘plash, saqlash va sud jarayonida qo‘llash uchun maxsus mexanizmlar yaratish ham muhim vazifa hisoblanadi. Xalqaro sud tizimini kiber jinoyatlar bo‘yicha maxsus ekspertiza bilan ta’minlash zarurati mavjud.

Xulosa qilib aytganda, kiber makonda qurolli mojarolar XGH uchun yangi imkoniyatlar va qiyinchiliklar yaratmoqda. Mavjud huquqiy bazani yangi texnologik sharoitlarga moslashtirib borish va zamonaviy urush usullariga mos keluvchi huquqiy mexanizmlar ishlab chiqish davr talabi hisoblanadi.

REFERENCE:

1. The Geneva conventions of 12 august 1949 // available at: https://www.icrc.org/sites/default/files/external/doc/en/assets/files/publications/icrc-002-0173.pdf
2. The official website: International Committee of the Red Cross, Cyber Warfare: does International Humanitarian Law apply? April 1, 2025. Available at: https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law
3. Zetter, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown Publishers, 2014: 156-189.
4. Lin, Herbert. Cyber Conflict and International Humanitarian Law. International Review of the Red Cross 94, no. 886 (2012): 515-531.
5. United Nations. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174, 2015.

6. Charter of the United Nations // http://treaties.un.org/doc/publication/ctc/uncharter.pdf
7. Haataja, S, The 2007 cyber-attacks against Estonia and international law on the use of force: an informational approach // https://research-repository.griffith.edu.au/server/api/core/bitstreams/e6e5408e-5ff9-5afb-bd29-e54ba1cc932b/content
8. Schmitt, Michael N. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press, 2013.
9. ICRC. International humanitarian law and the challenges of contemporary armed conflicts. Geneva: ICRC, 2019: 45-67.
10. Shackelford, Scott. (2012). Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Managing Cyber Attacks in International Law, Business, and Relations in Search of Cyber Peace. 1-393. 10.1017/CBO9781139021838.
11. Rid, Thomas. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies. 35. 5-32. 10.1080/01402390.2011.608939.
12. Dinstein, Yoram. The Conduct of Hostilities under the Law of International Armed Conflict. Cambridge: Cambridge University Press, 2016.
13. Benvenisti, Eyal. (2014). The Law of Global Governance. 10.1163/9789004279124.
14. Graham, David E. Cyber Threats and the Law of War. Journal of National Security Law & Policy 4, no. 1 (2010): 87-102.
15. Droege, Cordula. Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. International Review of the Red Cross 94, no. 886 (2012): 533-578.
16. ICRC. International humanitarian law and cyber operations during armed conflicts. Position Paper, Geneva: ICRC, 2019: 23-45.
17. Schmitt, Michael N., ed. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017
18. The White House. National Cyber Strategy of the United States of America. Washington D.C., 2018. // https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/
19. Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” Journal of Strategic Security, vol. 4, no. 2, 2011, pp. 49–60. JSTOR, http://www.jstor.org/stable/26463926.
20. Langner, Ralph. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy. 9. 49-51. 10.1109/MSP.2011.67.
21. Tsagourias, Nicholas, Cyber Attacks, Self-Defence and the Problem of Attribution (July 24, 2012). Journal of Conflict & Security Law (2012), Vol. 17 No. 2, 229–244, Available at SSRN: https://ssrn.com/abstract=253827