

37. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2025. április 22–24.
Nemzeti Közszolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar

Guns N' AI – Az autonóm fegyverrendszerek és a kiberfegyverek kiberbiztonsági kihívásai

Jelige: *Guns N' AI*

Pályamunka lezárásának időpontja: 2024. június.

2025.

Tartalomjegyzék

1	BEVEZETÉS	1
2	„CITIUS, ALTIUS, FORTIUS” – A FEJLŐDŐ KATONAI TECHNOLÓGIÁK ÉS A KATONAI KÉPESSÉGEK JAVÍTÁSA	3
2.1	A gyorsan fejlődő katonai technológiák – Mesterséges Intelligencia a hadseregben	4
3	AUTONÓM RENDSZEREK KÉRDÉSKÖRE	7
3.1	Az autonóm rendszerek működésének magyarázata.....	8
3.2	Mi az az autonóm fegyverrendszer? - Különbség automata, félautonóm, felügyelt autonóm és autonóm fegyverrendszerek között	10
4	AUTONÓMIA A KIBERTÉRBEN	14
4.1	Mi az a kiberfegyver és autonóm kiberfegyver?	14
5	AZ AUTONÓM FEGYVERRENDSZEREK KIBERBIZTONSÁGI KIHÍVÁSAI	17
5.1	Az autonóm fegyverrendszerek sebezhetőségei	18
5.2	Mesterséges intelligencia, mint kiberbiztonsági kockázat.....	19
5.3	Az autonóm fegyverrendszerek kiberbiztonságának megteremtése	22
5.4	Ha a kiberbiztonság megdől – Robotok a bíróság előtt?	25
6	AZ AUTONÓM FEGYVERRENDSZEREK ÉS A KIBERFEGYVEREK SZABÁLYOZÁSI KÉRDÉSEI.....	27
6.1	Autonóm fegyverek a humanitárius jog alapján - Az új szabályozási rendszer kialakításáért, valamint a betiltásukért vívott harc	28
6.2	A kiberfegyver szabályozási kérdései a humanitárius jog alapján.....	30
6.2.1	<i>Tallinn Manual 2.0 – Érvényesülhetne a nemzetközi jog a kibertérben?</i>	<i>32</i>
6.2.2	<i>Új egyezmény vagy a nemzetközi jog alkalmazása a kiberfegyverek szabályozása érdekében?</i>	<i>33</i>
7	EMPIRIKUS VIZSGÁLAT	36
7.1	Módszertan és hipotézis	36
7.2	Adatok ismertetése	38
7.3	Elemzés és eredmények.....	40
8	Összegzés	44
9	Irodalomjegyzék	46

1 BEVEZETÉS

A világ vezető pozíciójának betöltése mindig is egy stratégiailag meghatározó cél volt. Míg az ipari korszakban ehhez az acél és olaj járult hozzá, a jelenlegi adatvezérelt világunkban ezen pozíció megszerzéséhez úgy tűnik a mesterséges intelligencia a kulcs.

Nem túlzás azt állítani, hogy bárki is szerzi meg a vezető szerepet a mesterséges intelligencia terén, ő lesz a világ vezető hatalma. Éppen ezért, érthető az az elgondolás, hogy a „világ urát” a lehető legerősebb hadseregnek kell védelmeznie, így a hadiiparban elterjedt mesterséges intelligencia alkalmazása az elmúlt években új szintre lépett. Ez az új szint nem csupán a mesterséges intelligencia terén mutatkozik meg, ám kétségtelenül az első helyet foglalja el a gyorsan fejlődő katonai technológiák listáján. Az autonóm rendszerek elterjedése, egyre több és több kérdést vet fel, eddig még nem látott problémák elé állítva a szakembereket.

Az autonóm rendszerek olyan kiberbiztonsági kihívásokat jelentenek az egyes országok hadseregei számára, melyek nem csupán a technológia, de a jogi szabályozás terén is nehézségeket okoznak. Nehézségekbe ütközünk, amikor ezen rendszerek szabályozását vizsgáljuk, ugyanis a meglévő jogi normáknak bár érvényesülniük kellene, a fogalmi koncepciók hiánya nagyban megnehezíti ezt. Az egyes országok és szervezetek eltérően értelmezik az autonóm fegyver fogalmát, és ennek megfelelően különböző szinteken állnak a fejlesztés és alkalmazás terén. Ennek eredményeként előfordulhat, hogy a fegyverrendszereket félautonómnak vagy más, kevésbé pontos kifejezésekkel írják le, annak érdekében, hogy elkerüljék az abszolút autonóm címkét, és az ezzel együtt járó felelősséget. Azonban ez a megközelítés sem oldja fel teljesen a jogi és kiberbiztonsági aggályok, mivel végső soron nem számít, hogy egy rendszer, amely kibertámadás áldozata lesz, félautonóm vagy teljes mértékben autonóm volt-e. Az okozott károk ugyanis ugyanakkorák lehetnek, függetlenül attól, hogy milyen szinten áll a rendszer autonómiája.

Ezen rendszerek sebezhetősége megkérdőjelezhetetlen, s irányításuk átvétele beláthatatlan károkat okozhat. Mi a helyzet abban az esetben, ha egy autonóm fegyverrendszer kibertámadás következtében követ el jogellenes cselekedetet? Ki a felelős ilyenkor és ezt mi hivatott szabályozni? Az ilyen támadások hátterében sok esetben nemzetállamok vagy pedig nem állami szereplők állnak, s az így elkövetett támadások esetében már kiberműveletekről beszélhetünk. Ez pedig felvet egy újabb égető problémát, a kiberműveletek szabályozási kérdéseit.

A kiberműveletek során alkalmazott kiberfegyverek és szofisztikált támadások kihívás elé állítják a szakértőket a megfelelő szabályozás megteremtése terén. Évek óta zajlik a vita azt illetően, hogy a nemzetközi humanitárius jog alkalmazható-e a kiberműveletek tekintetében. A nemzetközi humanitárius jog hiányosságait megvizsgálva láthatjuk azt, hogy nem bizonyul minden esetben elégségesnek, sőt. A fizikai térben való alkalmazás is nehézségekbe ütközik, ám a kiberműveletek olyan szabályozási problémákat vetnek fel, melyekre a humanitárius jog jelenleg nem képes megoldással szolgálni. A probléma körbejárására a következő kutatási kérdést és hipotézist fogalmaztam meg: K1: Alkalmas a nemzetközi humanitárius jog arra, hogy szabályozza a kiberműveleteket? H1: A nemzetközi humanitárius jog önmagában nem elegendő ahhoz, hogy szabályozza a kiberműveleteket, különös tekintettel a kiberfegyverek kérdéskörére.

A jogi és kiberbiztonsági kihívásokra való minél hamarabbi problémamegoldás szükségességét az is alátámasztja, hogy mind az autonóm fegyverrendszerek, mind a kiberfegyverek részévé válnak a modern hadviselésnek. Ahhoz, hogy megállapítsam, hogy ezen technológiák esetlegesen a modern háborúk részévé válva nem minden esetben váltanak ki hatást, az orosz-ukrán háború során elkövetett három, autonóm képességekkel rendelkező dróntámadást és két jelentős kibertámadás hatásait vizsgáltam az érintett tőzsde és vállalatok részvényeinek vonatkozásában. A vizsgálat esetében a következő kutatási kérdést és hipotézist fogalmaztam meg: K2: Képesek-e befolyásolni az autonóm képességekkel rendelkező drónok által elkövetett támadások, valamint a kiberműveletek a tőzsde alakulását, hatást gyakorolnak-e a piacra, ezen események? H2: Az autonóm képességekkel rendelkező drónok általi támadások és kiberműveletek nem feltétlenül befolyásolják a piacot és nem minden esetben okoznak változást a részvények árfolyamában.

2 „CITIUS, ALTIUS, FORTIUS” – A FEJLŐDŐ KATONAI TECHNOLOGIÁK ÉS A KATONAI KÉPESSÉGEK JAVÍTÁSA

A katonai felszerelések modernizálása a hadseregek teljesítményének és képességének javításának egyik elengedhetetlen eleme, mely növeli a sikeres, kevesebb áldozattal járó küldetések esélyét. A „Citius, Altius, Fortius” – a latin kifejezés jelentése gyorsabban, magasabbra, erősebben – elve kiválóan tükrözi ezt a törekvést.

Az élesedő globális biztonsági környezetben a modern technológiák alkalmazása lehetővé teszi a hadseregek számára, hogy gyorsabban és hatékonyabban reagáljanak, magasabb szintű teljesítményt érjenek el, és erőteljesebben lépjenek fel a változó kihívásokkal szemben. Az innovatív technológiai fejlesztések a logisztikától a kommunikációig számos területen segítik a katonai műveleteket, hozzájárulva a modern és versenyképes védelmi stratégiák kialakításához. Az új technológiák stratégiai, operatív és taktikai szinten is jelentős mértékben képesek befolyásolni a képességeket (Billig & Graham et al., 2020).

Várhatóan a kialakulóban lévő technológiák minden harctéri szerepet és feladatot meg fognak változtatni. Valójában új feladatok jönnek létre, egyes régi feladatok megszűnnek, vagy legalábbis ritkábban kerülnek majd végrehajtásra, ami minden szinten megváltoztatja a katonai emberi teljesítményre vonatkozó követelményeket. A stratégiai szinten történő döntéshozatal során az automatizált segédeszközök lehetővé tehetik a döntések gyorsabb meghozatalát, csökkentve a kognitív munkaterhelést, ezzel javítva az irányítást. Bár a döntéseket a helyszínen lévő parancsnokok hozzák meg, a mesterséges intelligenciának köszönhetően a döntések meghozatalának gyorsasága nagy mértékben javulhat. A feltörekvő technológiák a döntéshozatal során olyan ajánlásokat tesznek, melyek részletesen levezetésre kerültek, s képesek folyamatosan értelmezni az áramló adatokat. A gép felvázolja az összes lehetséges döntési lehetőséget, ám meghagyja a mérlegelést az ember számára, akinek így gyorsabban van lehetősége a már meglévő ajánlásokat értékelni, s kiválasztani a szituációtól függő legjobbat (Billig & Graham et al., 2020).

Operatív szinten a feladatok általában a tervezést és az információszerzést - elemzést és - értelmezést jelentik. Az új technológiák pedig ezek hatékonyabb végrehajtását segítik. Lehetővé teszik a gépi és mélytanulást, mely új képességek kialakulásához is vezet. Az új eszközök lehetővé tennék többek között a pilóta nélküli légi rendszerek által távolról rögzített képek automatikus jellemzőinek kinyerését és osztályozását is (Billig & Graham et al., 2020).

Taktikai szinten a legfontosabb egyben legnehezebb megtalálni azon technológiákat, melyek a legnagyobb mértékben segítik a katonákat. Ez az a szint, ahol a katonák teljesítménye is szükségszerűen fejlődni fog annak érdekében, hogy az élvonalbeli csúcstechnológiákat teljes mértékben ki tudják használni az előnyök elérésének érdekében. Ebből kifolyólag is nagy hangsúly helyeződik arra, hogy a katonai emberi teljesítményt kutató közösségnek kritikus fontosságú szerepet kell játszania a legjobb technológiák gyors elfogadásának biztosításában. Ezen technológiák többek között segítenek a felderítésben és a veszélyes területeken végzett műveletekben. Az intelligens hálózatok, melyek összekapcsolják a katonai eszközöket és rendszereket, lehetővé teszik a valós idejű információcserét a harcmezőn, mely növeli a katonák helyzetérzékelését és az operatív hatékonyságot is (Billig & Graham et al., 2020).

Kétségtelen, hogy ezen technológiák eddig nem tapasztalt módon lesznek képesek javítani a harci képességeket, s többek között ezért is érdemes jobban megvizsgálni, hogy milyen technológiákkal is nézünk szembe pontosan.

2.1 A gyorsan fejlődő katonai technológiák – Mesterséges Intelligencia a hadseregben

Annak érdekében, hogy átfogó képet kapjunk a 10 legjelentősebb katonai technológiáról 2024-ben a StartUs 1036 globális startup and scaleup céget elemzett, melynek eredményeként elmondható, hogy a következő 10 technológia lesz kifejezetten meghatározó a katonai szektorban a következő években:

1. Mesterséges intelligencia
2. Fejlett védelmi berendezések
3. Robotika és autonóm rendszerek
4. A katonai dolgok internete (IoMT)
5. Kiberhadviselés
6. Virtuális valóság
7. Additív gyártás
8. Big Data és analitika
9. 5G összekapcsolhatóság
10. Blockchain

A mesterséges intelligencia nem csak azért kiemelkedő, mert az első helyet foglalja el a listán, hanem azért is, mert szinte minden utána felsorakoztatott technológia is igényli (igényelheti) valamilyen mértékben. Éppen ezért, jelen fejezetben a mesterséges intelligencia (MI) katonai felhasználása kerül bemutatásra (StartUs, 2023).

A mesterséges intelligenciát egy fajta „game-changer”-ként is említhetjük, hiszen ezen technológia egészen forradalmi megoldásokat kínál. Ez többek között annak köszönhető, hogy ebben az esetben egy olyan iparágról beszélhetünk, amely új fegyvereket és egyéb kiegészítő technológiákat is feltalál, a robotika és az autonóm rendszerek pedig olyan mértékben javítják a harci képességeket, amelyek képesek az iparág más trendjeire is hatást gyakorolni (StartUs, 2023).

A hatalmas adatmennyiség kezelése során fellépő nehézségek csak a hagyományos rendszereknek jelentenek problémát, a mesterséges intelligencia által vezérelt rendszerek hibázási lehetősége minimálisra csökkent. A döntéshozó képesség olyan rendkívüli fejlettségről ad számot, ami javítja a harci rendszerek önszabályozását, önellenőrzését, valamint önműködését is. A mesterséges intelligencia által a katonák gyorsabban felismerhetik a veszélyeket, valamint útmutatást kaphatnak a kezelésükhöz. Számos hadsereg repülőgépei és szárazföldi járművei rendelkeznek már ilyen jellegű intelligens vezérlőkkel, mely az egyik ideális példája a mesterséges intelligencia hadseregben való felhasználásának (Eliaçık, 2023).

A Boston Dynamics ékes példája annak az egyedi konstrukciónak, amely lehetővé teszi, hogy a robotok az emberek számára megközelíthetetlen terepeket hódítsanak meg, s képesek legyen bármilyen környezetben automatizált feladatokat végrehajtani. Ez nem csak azt bizonyítja, hogy bizonyos esetekben nincs is szükség az emberekre, hanem azt is, hogy az emberek biztonságát szolgálja az, ha egy harci környezetből kivonjuk az embert, és robottal helyettesítjük (Boston Dynamics, 2023). A pozitívumok mellett, amelyek egyre inkább erősítik a nemzeteket abban az elgondolásban, hogy rohamos tempóban fejlődjenek a mesterséges intelligencia terén, nem tud eltörpülni az a tény, hogy egy roppant költséges technológiáról beszélünk, ami egyre előkelőbb helyet foglal el egyes országok védelmi kiadásai között. Példának okán említhető az Egyesült Államok - aki nem melleleg élen is jár a technológia alkalmazásában - 2022-ben megközelítőleg 874 millió dollárt költött mesterséges intelligenciára (Keller, 2021).

A háborúban mindenki egyet akar, győzni, viszont a mai háborúkat nem lehet megnyerni a legújabb fegyverek, és legmodernebb rendszerek alkalmazása nélkül, melyek legalább részben

tartalmaznak mesterséges intelligencia komponenst. Éppen ezért számos példa figyelhető meg az elmúlt évekből, amikor ezen technológia bevetésre került a harctereken. Az egyik legaktuálisabb eset erre az orosz-ukrán háború. Ukrajna többek között használ török gyártmányú drónokat, melyeket kifejezetten az orosz katonai erők csapásmérésére és a rakétatámadásokra való válaszára rendeltek ki. Ezen drónok sebezhetősége megkérdőjelezhető volt, így ennek kiküszöbölésére amerikai gyártmányú páncéltörő rakétákat használnak annak érdekében, hogy meg tudják védeni a drónokat, valamint más haditechnikai eszközöket. Oroszország az egyik lefejlettebb drónokkal rendelkezik, melyek a lopakodó kialakításuknak köszönhetően képesek a radarok érzékelése nélkül repülni (Eliaçık, 2022).

Bár lehetne még sorolni azon hadi eszközöket, melyek esetében a mesterséges intelligencia alkalmazásával próbálnak a leghatékonyabban előnyre szert tenni a háborúban, a hangsúly elsősorban azon van, hogy már alkalmazzák ezeket az élvonalbeli technológiákat. Ez előfutára is lehet annak a ténynek, hogy a jövő háborúit kizárólag ezen technológiák alkalmazásával vívják majd.

3 AUTONÓM RENDSZEREK KÉRDÉSKÖRE

A mesterséges intelligencia felhasználása kifejezetten széleskörű, s mint említésre került korábban, szinte az összes feltörekvő katonai technológiának része. Nincs ez másként az autonóm rendszerek esetében sem, ahol ezen rendszerek funkcióinak végrehajtását a mesterséges intelligencia támogatja.

Amikor azt autonóm rendszerek kérdéskörét akarjuk körbejárni, akkor a legelőnyösebb, ha az elején, az autonómia fogalmának tisztázásánál kezdjük. Az autonómia tulajdonképpen a függetlenségnek azon szintje, melyet az emberek egy rendszernek biztosítanak egy adott feladat végrehajtásához. Az autonómia az automatizálás olyan spektrumára utal, amelyben független a döntéshozatal az adott feladattól, a kockázat szintjétől, valamint az ember-gép együttműködés mértékéhez igazítható (Chavannes, 2021). Az autonómia három egymástól eltérő koncepciót, mondhatni dimenziót ölel fel. A gép által végrehajtott feladat jellegét, az embert a végrehajtást végző géphez fűző viszonyát, valamint a gép döntéshozatalának fejlettségét. Attól függően, hogy az egyes dimenziókban mennyire fokozzák az autonómia mértékét, különböző típusú autonóm rendszereket különböztetünk meg: a félautonóm, a felügyelt autonóm, valamint a teljes mértékben autonóm rendszereket (Scharre, 2019).

Amikor az autonóm rendszerekről beszélünk akkor további fogalmak tisztázása elengedhetetlen, ugyanis a kérdéskör kifejezetten komplex. Az autonómiát a korábban ismertetett fogalom miatt is, elsősorban a robotokkal azonosítják. Ez nem áll messze a valóságtól, ugyanis létezik a robotika és autonóm rendszerek, mint kifejezés. A RAS (Robotic and Autonomous Systems) kiemeli a rendszerek fizikai (robotikus) és kognitív (autonóm) aspektusait. A RAS egy keretrendszer a robotikus és autonóm elemmel egyaránt rendelkező rendszerek leírására. Fontos kiemelni, hogy a RAS kifejezésben a „rendszerek” rész a fizikai rendszerekre utal (jelen dolgozat szempontjából: katonai rendszerek). A "robotikus" rész, amely a rendszer fizikai elrendezésére utal, azt jelenti, hogy a rendszer pilóta nélküli. Minden más fizikai szempont, mint méret, forma, repül-e, lebeg-e vagy gurul-e nyitva marad. Tehát a számítógépeken vagy hálózatokon futó automatizált szoftverrendszerek, beleértve a "botokat", azaz a szoftverek olyan darabjait, amelyek emberi beavatkozás nélkül képesek parancsokat végrehajtani, nem minősülnek RAS-nak, mivel fizikai komponensük nincsen. Így ezen botok „csupán” autonóm rendszernek minősülnek nem pedig robotikai rendszereknek (Chavannes, 2021).

Az autonóm rendszerek esetében létezik még egy olyan fogalom, melynek ismertetése elengedhetetlen. Bár a mesterséges intelligencia katonai felhasználásának bemutatása kifejezetten pozitívnak hatott, az autonóm rendszerekben való működésük határozottan hagy kivetnivalót maga után. Ugyanis, ha a háború könyörtelensége párosul a jelenleg még kiaknázatlan lehetőségekkel, melyeket a mesterséges intelligencia magában rejt, akkor a robotokkal és egyéb autonóm rendszerekkel vívott háborúk társadalmi és gazdasági katasztrófákhoz vezethetnek. Ez a megállapítás maga után vonza a halálos autonóm fegyverrendszerek (Lerthal Autonomus Weapon System – LAWS) fogalmát. Ebben az esetben olyan rendszerekről beszélünk, melyek emberi beavatkozás nélkül választják ki a bizonyos előre meghatározott célpontokat, miután az ember úgy döntött, beveti az adott rendszert azzal a tudattal, hogy a támadás elindítása után emberi beavatkozással és emberi erővel a rendszert már nem lehet megállítani (Chavannes, 2021).

3.1 Az autonóm rendszerek működésének magyarázata

Ahhoz, hogy az autonóm rendszerek kihívásait és kockázatait azonosítani tudjuk, ezzel meghatározva mindazt, melyre fel kell készülnünk ezen rendszerek elterjedése esetén, elengedhetetlen, hogy megértsük és átlássuk a működésüket. Tekintve, hogy a katonai felhasználású autonóm rendszerek működéséről nincsenek ismereteink, így a rendszerek működése általánosságban kerül bemutatásra.

Az autonóm rendszer a hálózatiépítésben egy vagy több kapcsolódó IP-előtaggal rendelkezik, amely szabályozza, hogy az autonóm rendszer hogyan cserél útválasztási információkat egyéb autonóm rendszerekkel. Az autonóm rendszereket az különbözteti meg más hálózati csoportoktól, hogy a külső autonóm rendszerek számára úgy kell tünnie, hogy a rendszer egyetlen, összefüggő útválasztási tervvel rendelkezik, attól függetlenül, hogy a rendszeren belüli kommunikáció hogyan történik. Az autonóm rendszerek útválasztási információkat cserélnek az útválasztási irányelveik alapján, és minden kapcsolódó rendszer ellenőrzi az IP-előtagjai által meghatározott IP-címtartományt. Ily módon az egyik hálózatban lévő eszköz adatcsomagokat cserélhet egy másik hálózatban lévő eszközzel. Nézzük meg a következő példát. Az AS1 autonóm rendszer tartalmazza a NET1 hálózatot, az AS2 autonóm rendszer pedig a NET2 hálózatot. Miután az AS1 és az AS2 útválasztási információkat cserél és kapcsolatot létesít, a NET1 hálózaton lévő számítógép adatcsomagokat cserélhet a NET2

hálózaton lévő számítógéppel. Az autonóm rendszerek általában három kategóriába sorolhatóak:

1. Multihomed: Egy olyan autonóm rendszer, amely két vagy több autonóm rendszerrel van összeköttetésben.
2. Tranzit: Egy olyan kapcsolódó rendszer, amely két vagy több külső autonóm rendszer közötti összeköttetésként működik.
3. Single-homed: Ez egy olyan kapcsolódó rendszer, amely csak egy külső kapcsolódó rendszerrel van összeköttetésben.

Minden autonóm rendszer egy globálisan egyedi számot kap, amelyet autonóm rendszerszámnak (ASN) neveznek. A szám az autonóm rendszer azonosítójaként szolgál, és az útválasztási információk más autonóm rendszerekkel való cseréje során szükséges. Az autonóm rendszerek belső hálózatai egy vagy több belső átjáró protokoll segítségével kommunikálnak egymással, megosztva az útválasztási információkat. Azonban az autonóm rendszerek közötti kommunikáció más megközelítést alkalmaz, mivel egyetlen külső átjáró protokollra, a Border Gateway Protocol (BGP)-re támaszkodik. Ez a protokoll lehetővé teszi az útválasztási információk cseréjét és az adatsomagok hatékony továbbítását az autonóm rendszerek között. A BGP az internetet működtető útválasztási protokollként is ismert, mivel kulcsszerepet játszik az autonóm rendszerek közötti hálózati elérhetőségi információk közvetítésében. A BGP egy autonóm rendszerek közötti útválasztási protokoll, amely lehetővé teszi a BGP-rendszerek közötti hálózati elérhetőségi információk cseréjét. Ezen információk alapján a BGP optimalizálja a csomagok útvonalát a cél autonóm rendszerek irányába. A protokoll a TCP (Transmission Control Protocol) protokollt használja szállítási protokollként, aminek köszönhetően kompatibilis az internet többi részével, és nem igényel olyan műveleteket, mint az explicit szekvenálás vagy az újra küldés. Amikor két eszköz között TCP-kapcsolat jön létre, a két eszköz üzeneteket cserél a kapcsolati paraméterek megerősítésének érdekében. Az autonóm rendszer a BGP-t használják arra, hogy bejelentsen, mely autonóm rendszerekhez tud csatlakozni, és mely IP-címekért felelős a rendszer. A BGP-kommunikációban részt vevő útválasztók folyamatosan frissítik egymást a legfrissebb útválasztási információkkal. Minden BGP-router egy útválasztási táblát tart fenn ezen információk tárolására. A BGP ezt az információt - az ASN-ekkel együtt - felhasználhatja egy olyan továbbítási topológia kialakításához, amely a csomagokat a legjobb útvonalak mentén irányítja, miközben elkerüli a hálózati hurkokat. A protokoll a célállomás-alapú továbbítási paradigmát követi, amelyben az útválasztó csak az IP-fejlécben szereplő célcím alapján továbbítja a csomagot. Ennek

eredményeképpen az útválasztási szabályoknak meg kell felelniük ennek a paradigmának (Sheldon, 2023).

3.2 Mi az az autonóm fegyverrendszer? - Különbség automata, félautonóm, felügyelt autonóm és autonóm fegyverrendszerek között

Az autonóm fegyverek az autonóm rendszerek egy olyan alcsoportját képezik, melyek kifejezetten katonai alkalmazásban való használatra lettek tervezve. Tehát, egy kisebb, de egy jelentősen specifikus része az autonóm rendszereknek a biztonsági és védelmi kontextusban. Az autonóm fegyvereknek olyan specifikus feladataik vannak, mint a célpontok azonosítása és a támadás végrehajtása, míg az általánosságban vett autonóm rendszerek más célokat is szolgálhatnak, iparágaktól függően. Ahhoz, hogy az autonóm fegyver fogalmát körbejárjuk elengedhetetlen az automata, félautonóm, felügyelt autonóm és az autonóm rendszerek közötti különbség megértése is, majd pedig ugyanezen elvek mentén működő fegyverrendszerek elhatárolása (Scharre, 2019).

Az automata rendszerek egyszerű gépek, amelyek nem hoznak döntéseket, viszont érzékelik a környezetet és cselekednek, ám az érzékelés és a cselekvés közötti kapcsolat lineáris és azonnali, valamint nagyrészt kiszámítható az emberi felhasználó számára. Egyik legjobb példa az automata rendszerekre a termosztát. A felhasználó beállítja a kívánt hőfokot, a rendszer pedig érzékeli, amikor a hőmérséklet eltérő a beállított értéktől, így a termosztát bekapcsolja a fűtést vagy éppen leállítja azt. Az ilyen rendszerek működése egyszerű és küszöbalapú (Scharre, 2019).

Az autonóm rendszerek esetében több típust különböztetünk meg, a félautonóm, a felügyelt autonóm és az autonóm rendszereket. A félautonóm rendszerek esetében az ember a ciklusban tartózkodik. Az ilyen rendszerekben a gép végrehajt egy feladatot, ám mielőtt tovább folytatná, megvárja, hogy az ember, aki a ciklusban lévő felhasználóként van jelen cselekedjen. Ezek a rendszerek végig haladnak az OODA cikluson¹ viszont a ciklust megtöri az ember. A rendszer

¹ Az OODA ciklus (Observe, Orient, Decide, Act) a döntéshozatal négylépcsős megközelítése, amely a rendelkezésre álló információk szűrésére, kontextusba helyezésére és a legmegfelelőbb döntés gyors meghozatalára összpontosít, miközben a rendelkezésre álló adatok bővülésével változtatásokat lehet végrehajtani. Eredetileg arra használták, hogy a katonákat kiképezzék, a gyors időérzékeny döntések meghozatalára, amikor nincs idő minden információ összegyűjtésére. A stratégia célja az volt, hogy az OODA-ciklus folyamatát gyorsabban hajtsák végre, mint az ellenfél, hogy beszivárognak és megzavarják az ellenség döntési ciklusát (Lewis, 2023).

képes a környezet észlelésére, és ez alapján javasolhat akciókat, ám végre nem hajtja azt emberi jóváhagyás nélkül. A gép komplex és szabályalapon működik (Scharre, 2019).

A felügyelt autonóm rendszerek esetében az ember a cikluson helyezkedik el, mondhatni a ciklus tetején „ül”. Az üzembe helyezés után a gép képes önálló érzékelésre és cselekedni is tud, ám az emberi felhasználó felügyeli a műveletet és szükség esetén közbe tud lépni. Azonban fontos kiemelni azt, hogy a felhasználó nem minden esetben képes az időben történő beavatkozásra (Scharre, 2019).

A teljes mértékben autonóm rendszerek esetében pedig az ember a cikluson kívül van. Ezen rendszerek az emberi beavatkozás nélkül képesek érzékelni, dönteni és cselekedni. Miután a gép aktiválásra kerül, az mindenfajta kommunikáció nélkül hajtja végre a feladatot. Az ilyen rendszernek a belső kognitív folyamatai gyakran annyira fejlettek, hogy az emberi felhasználónak kifejezetten nehézséget okoz átlátni rajtuk, sok esetben szint lehetetlen. Az érthető, hogy a rendszer éppen milyen feladatot hajt végre, ám az, hogy ezt milyen módon teszi meg, az kérdéses. Éppen ezért is hivatkoznak az ilyen rendszerekre sokszor célorientáltként, ami tulajdonképpen azt jelenti, hogy bár az emberi felhasználó szabja meg a célt, a gép rugalmasan, a célnak megfelelően dönti el, hogy mit tesz meg annak elérése érdekében (Scharre, 2019).

Bár elméletben az elhatárolás az említettek alapján történik, fontos kiemelni, hogy a gyakorlatban homályosak az automatizált és autonóm rendszerek közötti választvonalak. Az autonóm kifejezést sokszor a jövőbeli még nem elkészült rendszerekre használják, ám amint ezek létrejönnek, az emberek már „automatizáltként” jellemzik őket. Kicsit hasonló ez a mesterséges intelligencia esetében is, ahol a gépek által még végre nem hajtott feladatok kapcsán alkalmazzák az MI kifejezést, ám amint a gép sikerrel jár a végrehajtás során, már csak egyszerű „szoftverként” hivatkoznak rá (Scharre, 2019). Nehézségekbe ütközünk az elhatárolás esetében azért is, mert az egyes országok és szervezetek eltérően értelmezik az autonóm rendszer, valamint fegyver fogalmát, és ennek megfelelően különböző szinteken állnak a fejlesztés és alkalmazás terén. Ennek eredményeként előfordulhat, hogy a fegyverrendszereket félautonómnak vagy más, kevésbé pontos kifejezésekkel írják le, annak érdekében, hogy elkerüljék az abszolút autonóm címkét, és az ezzel járó felelősséget.

Az autonómia nem azt jelenti, hogy a rendszer szabad akarattal rendelkezik vagy nem engedelmeskedik egy adott programozásnak. A különbség abban áll, hogy amíg egy automatikus rendszer esetében a lineáris kapcsolat van az érzékelés és a végrehajtás között, addig az autonóm rendszerek egy sor változót vesznek figyelembe annak érdekében, hogy

képesek legyenek a leghatásosabb cselekvés megállapítására. A célorientált viselkedés egy ellenőrizetlen környezetben kulcsfontosságú a rendszer számára, hiszen a bonyolultabb környezetben a bonyolultabb feladatok esetében létfontosságú, (hiszen ilyen környezetben való bevetésre is tervezték őket) hogy a gép képes legyen az adott szituációnak megfelelően dönteni (Scharre, 2019).

A fegyverrendszerek pontosan ugyanezt a logikát követik. A fegyverrendszer egy ellenséges célpontok után kutató érzékelőből, egy, a célpont megtámadását eldöntő döntéshozatali elemből és lőszerből áll. A fegyverrendszer néha egyetlen platformból áll, például egy repülőgép esetében. A radar a célpont után kutat majd érzékeli azt, az ember döntést hoz a támadásról majd a rakéta végrehajtja azt. Más esetekben a fegyverrendszer több fizikai platformon kerülhet elosztásra. Egy tengeri járőr repülő észlelhet egy ellenséges hajót, majd ezt az információt továbbadja egy közeli baráti hajónak, amely kilövi a rakétát. A védelmi stratégiák ezeket a megoldásokat nevezik harci hálózathoz (Scharre, 2019).

Automata fegyverek a géppuskák. Az automata fegyverek egészen addig lőnek, amíg az elsütőbillentyű meghúzva marad. A modern géppuskák számtalan alakban léteznek, a biztonsági őrként általánosan használt fegyverektől kezdve egészen az egy percenként több ezer lövedéket kilövő masszív gépágyúig. Ám az, hogy milyen alakban léteznek szinte lényegtelen, amint elsütésre kerülnek az erejük kézzelfoghatóvá válik (Scharre, 2019).

Az autonóm fegyverek esetében szintén félautonóm, felügyelt autonóm és teljes mértékben autonóm fegyverrendszereket különböztetünk meg. A logika szinte ugyanaz, mint a rendszerek esetében. A félautonóm fegyver esetében az ember ugyanúgy a ciklusban helyezkedik el, emberek döntenek el, hogy megtámadják-e az adott célpontot. Napjainkban elmondható, hogy a legtöbb fegyver félautonóm, ám néhány esetben átlépik az autonóm fegyverek közötti válaszvonalat. A felügyelt autonóm fegyverek esetében az ember a cikluson helyezkedik el. Jelenleg legalább 30 ország használ felügyelt autonóm fegyvereket a hajók, bázisok és különböző járművek védelmének érdekében. Az üzemmódba helyezett és aktivált rendszerek önállóan, emberi beavatkozás nélkül támadják meg a közeledő rakétákat, lövedékeket, ám ezt az ember valós időben képes ellenőrizni. A felügyelt autonóm fegyverek fontossága abban az esetben mutatkozik meg, amikor a harci cselekmények sebessége túlterheli az emberi operátorokat. A teljes mértékben autonóm fegyverrendszerek nem mondhatóak elterjedtnek, ám bizonyos rendszerek átlépik az autonómiába vezető határt. Ezek a fegyverek aktiválásuk után képesek a célpontok kutatására, azok érzékelésére a támadás eldöntésére, s magára a támadás végrehajtására. Az ember, mint felhasználó képtelen az aktiválás után a beavatkozásra. Ilyen

például az izraeli Harpy, amelyet több országnak, köztük Chilének, Dél-Koreának, Indiának, Kínának, és Törökországnak is eladtak már. Ez egy olyan vándorló lövedék, amely képes önállóan kutatni, érzékelni és megtámadni a kiválasztott célpontot. Az emberi felhasználó csupán azt adja meg, hogy a Harpy pusztítsa el bármelyik radart a térségben, adott időben, viszont azt a Harpy dönti el, hogy melyik lesz a konkrét radar (Scharre, 2019).

Ha úgy gondoljuk korai még erről beszélni és az autonóm fegyverek kérdésköre még a távoli jövő, akkor érdemes szem előtt tartani az információt, hogy 1980-as évek során az amerikai haditengerészet már kifejlesztett egy olyan vándorló lövedéket, amely önállóan képes volt kutatni, érzékelni és végrehajtani a támadást a szovjet hajók ellen (Scharre, 2019).

4 AUTONÓMIA A KIBERTÉRBEN

A korábbiakban bemutatott autonóm megoldások nem csak a fizikai térben, de a kibertérben is megvalósulhatnak és egyre elterjedtebbnek bizonyulnak. A kibertér szereplői között lehetnek automatizált módon működő, de valós szereplők által irányított, vagy akár autonóm módon működő szintetikus szereplők is. Továbbá a kibertérben autonóm módon működő, valós karakterek vagy programok által alkotott digitális entitások (például mesterséges intelligencia alapú szereplők vagy robotok) is létezhetnek. A digitális és valós karakterek közötti kapcsolat nem mindig egyértelmű vagy könnyen azonosítható. Továbbá egy valós karakterhez több digitális karakter is kapcsolódhat, és egy digitális karakterhez is tartozhat több valós karakter (Munk, 2018).

Az autonómia a kibervédelem esetében kulcsfontosságú tényező, hiszen számos kibervédelmi megoldás megvalósítását könnyíti meg az autonóm módon való működés. A támadások óriási száma miatt lehetetlen vállalás az összes kiszűrése, hiszen néhány elkerülhetetlen módon hatol át a védelmen. A nulladik napi sérülékenységek kihasználása, a nem frissített rendszerek, fertőzött USB meghajtó gépbe helyezése, a rosszindulatú hivatkozásra kattintó felhasználók mind olyan veszélyeket jelentenek, melyek ellen hiába építettünk ki szilárd védelmet, az bármikor megdőlhet. Mindez azt jelenti, hogy az aktív kibervédelem elengedhetetlen a hatékony védekezésben, amely a rosszindulatú programok után kutat a hálózaton, eltávolítja azokat, majd pedig frissíti a hálózatot. Az összes hálózat naprakészen tartása szinte lehetetlen, az összes sérülékenység elleni frissítés manuális úton kifejezetten időigényes. Éppen ezért olyan automatizált rendszerekre van szükség, amely során az embert kivesszük a ciklusból (Scharre, 2019).

Mindazonáltal, a kibertérben megjelenő autonómia nem csak a védekező feleket mozgatja, de bizony a támadókat is, így a kibertér és a korábbiakban felvázolt autonóm fegyverek több ponton is összeérnek, valamint megjelenik a kiberfegyverek kérdésköre is.

4.1 Mi az a kiberfegyver és autonóm kiberfegyver?

A kiberfegyver pontos és átfogó meghatározására még nem született egy általánosan elfogadott fogalom, hiszen egy összetett kifejezésről beszélünk. Mivel ezen kibertechnológia általában kettős funkciókat tölt be – támadás-védekezés, békés-agresszív, legális-illegális, - így további bonyodalmakat okoz a meghatározása. A bonyodalmat tovább erősíti, hogy az egyébként

jogszerű egyedi szoftvereszközök zavaró vagy pusztító célokra is alkalmazhatók. Ebből kifolyólag a kiberfegyver meghatározása többféleképpen is megvalósulhat. Érthetünk ez alatt olyan szoftvereket és informatikai rendszereket (IT), amelyek az IKT-hálózatokon keresztül képesek pusztító hatást kiváltani, és amelyeknek ez az elsődleges és egyben egyetlen felhasználási módja. Ebben az esetben a kiberfegyverek egy szűkebb meghatározásáról beszélünk, melyben a fő szempont, hogy az IT rendszerek nem önálló fegyverek, hanem egy tágabb értelemben vett fegyverbe kell őket beépíteni. Tehát ezen meghatározás alapján csak akkor van szó tényleges kiberfegyverről, ha a szoftver vagy az IT-rendszer kizárólag csak pusztító célra használható. A másik meghatározás alapján olyan szoftverek és informatikai rendszerekről beszélünk, amelyek az IKT-hálózatokon keresztül képesek manipulálni, megzavarni, vagy akár megsemmisíteni a célzott információs rendszereket és hálózatokat. Ennek a meghatározásnak az az előnye, hogy a tágabb fogalommeghatározással szemben minden olyan eszközre kiterjed, amelyet támadó kibertevékenységekben fel lehet használni (Miralis, 2023).

A fogalmat tovább árnyalja, hogy egy ideje megjelent az autonóm kiberfegyver fogalma is. A mesterséges intelligencia, a gépi tanulás és a fejlett rosszindulatú programkódolási technikák fejlődése a kiberfegyverek új fajtáját hozták létre, amely bizonyos szintű intelligenciával képes működni. Ezek az autonóm kiberfegyverek képesek megkeresni saját célpontjaikat és azonosítani az egyedi támadási vektorokat. Az offenzív kiberműveletek terén elért eredményeket a kibervédelem autonómiájában és intelligenciájában elért azonos fejlődéssel párosítják. Az automatizált rosszindulatú programok legegyszerűbb formáját „féregnek” nevezik, amely vakon replikálja magát a számítógépek hálózatán keresztül, előre meghatározott kódolt utasítások sorozatát hajtva végre, mint például a spam megjelenítése vagy a fájlrendszerek titkosítása a felhasználók kizárása érdekében. A modern rosszindulatú programok ügyessé váltak önmaguk elhomályosításában, hogy elkerüljék a víruskereső és más kiberbiztonsági rendszerek általi észlelést azáltal, hogy számos fejlett kódfordítási technikát alkalmaznak. Ez a „polimorf” kártevő gyakran tartalmaz egy titkosított mutációs motort, így a vírus hash aláírása akár 10 percenként is megváltozhat. Egy fejlettebb technika a „metamorf” kártevők használata, amelyek alapvetően átírják magukat, és véletlenszerű kódszegmenseket adnak hozzá, vagy átrendezik a belső funkcióit, hogy minden alkalommal teljesen más programként jelenjen meg. Ez a technika különösen veszélyes zsarolóvírus-fertőzések esetén, mivel a rosszindulatú program minden egyes új fertőzés esetén újraírja magát (Ari, 2023).

A Stuxnet egyike a legjelentősebb kibertámadásoknak melyek súlyos károkat okoztak, ezért többek között kiberfegyverként is jellemezték. Ezen túlmenően pedig a beavatkozás nélküli, független működése miatt a Stuxnetet autonóm kiberfegyverként is megjelölték. Az azonban nem világos, hogy ebben az értelemben az autonómia csak a teljesen autonóm kiberrendszerekre vonatkozik-e, vagy a fejlett automatizált rendszer bizonyos értelemben szintén autonómnak tekinthető-e. A teljesen autonóm rendszerek, amelyek képesek önmagukat aktiválni, (újra)programozni, ezáltal teljesen helyettesítve az embert még messze van a létezésről. Mindazonáltal elmondható, hogy fokozódik a kiberképességek automatizálása, mely egyre közelebb visz minket az eddig még nem látott kiberbiztonsági kihívásokhoz (Perez, 2023).

5 AZ AUTONÓM FEGYVERRENDSZEREK KIBERBIZTONSÁGI KIHÍVÁSAI

A kiberfegyverek kérdéskörének megvizsgálása után nézzük meg az autonóm fegyverrendszerek kiberbiztonsági kihívásait.

A rendszerek növekvő autonómiája bár előrelépést jelent a modern hadviselés terén, egyúttal súlyos kihívások elé is állít minket a kiberbiztonság szempontjából. Az autonóm fegyverrendszerek kiberbiztonságának megőrzése nem csupán technikai kihívásokkal jár, hanem komoly stratégiai és etikai dilemmákat is felvet. Ha valaki képes lenne átvenni az irányítást ezen rendszerek felett, a következmények beláthatatlanok lehetnek. Az elszabadult robotok vagy rosszindulatú irányítás alatt álló fegyverek szenáriói már régóta foglalkoztatják a szakértőket és etikai gondolkodókat egyaránt. Egy kibertámadás során az autonóm fegyverek feletti irányítás átvételével súlyos károk és veszteségek okozhatók, ezzel akár életveszélyes helyzeteket is teremtve. Az autonóm fegyverrendszerek kiberbiztonságának fenntartása és az ezekkel kapcsolatos szabályozási kihívások kezelése kulcsfontosságúvá vált annak érdekében, hogy keretet szabjunk a modern hadviselésnek.

Már 2011-ben az Egyesült Államok által használt RQ-170 Sentinel lopakodó pilóta nélküli megfigyelő repülőgép elfogása is rávilágított az ellenséges környezetben működő autonóm rendszerek előtt álló kihívásokra. A nyilvános jelentések alapján ugyan csak találgatni lehet azt illetően, hogy hogyan történt az elfogás, a hiteles jelentések szerint azonban ezt az RQ-170-est Irán nukleáris fegyverfejlesztési programjának megfigyelése során fogták el. Mivel a fényképeken látható volt, hogy a repülőgépváz sértetlen maradt, valószínűsíthető, hogy nem lőtték le. Ebből kifolyólag feltételezhető, hogy zavarták, eltérítették a rendszert, így kényszerleszállást hajtott végre (Madan et al., 2016).

A helyzet azóta még jelentősebbé nőtt ki magát, hiszen napjainkban egyre több autonóm képességekkel rendelkező fegyver kap szerepet a harctereken. Habár nem lehet egyértelműen kijelenteni, hogy csak autonóm rendszerek ezek, de az biztos, hogy rendelkeznek autonóm képességekkel. Az orosz-ukrán háború során is több, autonóm képességekkel rendelkező drónt kaptak el. 2024 februárjában az ukrán katonák figyelemreméltó bravúrt értek el az Orlan-30 néven ismert orosz felderítő pilóta nélküli légi jármű elfogásával. A gépnek kényszerleszállást kellett végrehajtani a zavarásnak köszönhetően (Malyasov, 2024).

Az autonóm fegyverrendszerek és hozzájuk hasonló technológiák, mindig magukban hordozzák az új sebezhetőségeket, illetve a már meglévő sebezhetőségek újszerű kihasználását.

Minden, ami szoftveren fut, az támadható vagy manipulálható. Ez fokozottan igaz azon rendszerekre, melyek olyan komplexitással rendelkeznek, mint az autonóm fegyverrendszerek.

5.1 Az autonóm fegyverrendszerek sebezhetőségei

Mivel ezen autonóm rendszerek célja, hogy egyre inkább egy kommunikációtól elzárt környezetben működjenek, így nehézséget okoz annak megállapítása, hogy a fegyverrendszer veszélybe került-e, vagy a beprogramozott parancsoknak megfelelően működik-e. Amikor kiberbiztonsági kockázatokról beszélünk, éppen emiatt az ilyen rendszer esetében, az elsődleges és legnagyobb problémát a nulladik napi sérülékenységek jelentik. Példának okán említhető a "Heartbleed" sebezhetőség, mely közel két és fél évig létezett a világ számos számítógépes rendszerében, mielőtt felfedezték volna. Elemzők véleménye szerint az ilyen hibák tíz hónapig is észrevétlenek maradhatnak, mielőtt felfedezik és kijavítják őket, így a rosszindulatú szándékkal rendelkezők számos lehetőséget kapnak arra, hogy pusztítást végezzenek a rendszerekben, mielőtt új sebezhetőségeket használnának ki. Az ilyen rendszerek esetében sokszor a fejlesztők sem tudják, hogy a rendszer mi alapján hajtja végre az utasításokat, így az ezzel kapcsolatos sebezhetőségek ismerete is hiányos. Az egyre inkább autonóm képességekkel rendelkező rendszerek bevetési ideje is kockázatot jelenthet. Minél hosszabb ideig áll egy rendszer üzemképesen, de bevetés nélkül, annál több ideje van a támadónak újabb és újabb sebezhetőségek felfedezésére. Bár ebben az esetben nem szükséges egyből a támadóra gondolni. Kérdés tárgyát képezi, hogy amennyiben a rendszert üzemeltetők fedeznek fel sérülékenységet, mely azonnali javítást igényel egy olyan rendszer esetében, mely már üzembe helyezésre került egy korlátozott kommunikációval rendelkező környezetben, milyen javítási lehetőségek állnak rendelkezésre. Lehetséges a sebezhetőség távoli javítása, vagy legalább egy hibabiztos leállítási mód elindítása (Unidir, 2017)?

A félautonóm és a felügyelt autonóm fegyverrendszerek esetében ez lehetséges, hiszen előbbi esetben az ember a ciklusban míg utóbbi esetben az ember a cikluson helyezkedik el. Mivel az ember, aki felügyeli, a rendszerrel egy helyen helyezkedik el, így fizikai módon is ki tudja kapcsolni, ha a rendszer nem reagál az utasításokra. A teljes mértékig autonóm fegyverrendszerek esetében ez nem mondható el, hiszen ezen rendszer mögött meghúzódó működési logika pontosan az, hogy az aktiválás után az ember, mint felhasználó képtelenné válik a beavatkozásra (Scharre, 2019).

5.2 Mesterséges intelligencia, mint kiberbiztonsági kockázat

A mesterséges intelligencia, önmagában kiberbiztonsági kockázatot jelent. Lehetetlen vállalás egy olyan rendszer számára biztonságot kialakítani, amely sok szempontból olyan eredményeket hoz, melyek jelenleg érthetetlenek még a tervezői számára is. A mesterséges intelligencia abban az esetben is képes váratlanul viselkedni, ha az ember szükség esetén be tud avatkozni. A váratlan lépések önmagukban nem jelentenek rosszat, ez is része a mesterséges intelligencia erősségének, hiszen ezek kreatív problémamegoldást jelentenek. A probléma abban rejlik, hogy egy felügyelt rendszer esetében, az embereket nem lehet előre felkészíteni ezen kreatív problémamegoldások megítélésére. Nem fogják tudni eldönteni, hogy az autonóm funkciókkal rendelkező fegyverrendszer a tervezettől eltérő módon viselkedik-e – akár belső hiba, akár rosszindulatú beavatkozás miatt - vagy pedig csak kreatív megoldást alkalmaz. Ez egyértelműen a csökkenti a megfigyelő beavatkozási képességét, és növeli a kiberbiztonsági kockázatokat is (Unidir, 2017).

A katonai alkalmazásokban használt mesterséges intelligencia jelentős mértékben nagy mennyiségű adatra támaszkodik. Ezek az adatok, megfelelő védelem hiányában sebezhetővé válhatnak. Az MI-rendszerek megzavarását célzó kibertámadások veszélyeztethetik a kritikus fontosságú műveleteket, és beláthatatlan következményekkel járhatnak (LinkedIn, 2023).

A mesterséges intelligencia behozza a gépi tanulás problematikáját is. Egyre nagyobb az érdeklődés az autonóm fegyverrendszerek esetében a gépi tanulás irányába, mely ugyanúgy mesterséges intelligenciaként tartható számon. A gépi tanulásnak önmagában is vannak kockázatai, ám ugyanakkor ezek a mesterséges intelligencia kockázataiként is értelmezhetők (ICRC, 2022).

Az autonóm fegyverrendszerek és a kibernműveletek közötti talán legsúlyosabb kölcsönhatás az lenne, ha a gépi tanulást nemkívánatos vagy akár jogellenes hatás kiváltására használnák. Számos módja lehet annak, hogy az ilyen rendszereket, az eredetileg beprogramozott módtól eltérítsék kibernműveleteken keresztül (Unidir, 2017). Az egyik ilyen módszer az adatmérgezés. Ahhoz, hogy egy gép felismerje, hogy egy harckocsi áll vele szemben, melyet meg kell támadnia, nemcsak az összes érintett járműről kell képeket gyűjteni, de ezt különféle körülmények között –változó fényben, eltérő szögben - is szükséges megtenni. Az adatokat ezután adatelemzők készítik elő az MI-rendszer betanítása érdekében. A mesterséges intelligencia-rendszer kifejlesztéséhez szükséges adatmennyiség azonban nagy mértékű sebezhetőséget okoz. Az adatok mennyisége feltételezi, hogy az elemzőknek nincs lehetőségük

ellenőrizni, hogy minden egyes összegyűjtött kép valódi ellenséges páncélozott jármű-e, vagy hogy a képek a páncélozott járműtípusok teljes skáláját reprezentálják. Így ez az első pont, ahol az ellenség megtámadhatja a rendszert mérgezéssel. A mérgezés célja az MI-rendszer által tanulás során felhasznált adatok megváltoztatása, annak érdekében, hogy a rendszer által tanult adatok hibásak legyenek. Ez a folyamat megtámadja a rendszer integritását, még mielőtt az működésbe lépne. Kulcsfontosságú, hogy a rendszer helyes tanulása biztosítva legyen. Az adatok részletes kezelése segíthet csökkenteni a kockázatokat, bár idő- és erőforrás igényes. A műszaki vezérlők megfelelő elhelyezése és a jól képzett személyzet a mesterséges intelligencia életciklusának minden szakaszában a ciklusban maradva csökkentheti a mérgezéssel járó támadások kockázatát (Starck et al., 2022).

A gépi tanulás számos egyéb támadási formának is kitett, melyek veszélyeztetik az autonóm rendszerek teljesítményét, megbízhatóságát és biztonságát. Az ellenséges támadások gépi manipulációs formája, más néven a kizárás célja a gépi tanulási modell kimenetének megváltoztatása a bemeneti adatok finom, de rosszindulatú megváltoztatásával (LinkedIn, 2024). Az ilyen jellegű támadások köthetők az arcfelismeréshez, tárgyfelismeréshez vagy célfelismeréshez. Az kizárási technika magában foglalja bizonyos képpontok színének enyhe módosítását, ezáltal befolyásolja azt, hogy hogyan alkalmazza a rendszer a tanultakat. Az emberi szem számára szinte változatlan képet az MI tévesen minősítheti. Ennek a technikának hatásait a kutatók mutatták be, amikor a mesterséges intelligenciának - amely korábban helyesen azonosította egy panda képét - ugyanazt a képet mutatták be, de a képhez hozzáadott színekkel manipulálták, amelyek az emberi szem számára észrevehetetlenek. A mesterséges intelligencia nemcsak, hogy gibbonként azonosította a pandát, de mindezt rendkívül nagy magabiztossággal tette. Az a támadó, aki hozzáfér a rendszer kimeneteihez vagy előrejelzéseéhez, robusztusabb vagy célzottabb kizárási módszert dolgozhat ki. Az ilyen támadások a legszélesebb körben kutatott ellenséges módszerek közé tartoznak, így az összes lehetséges támadási lehetőség elleni védekezés kihívást jelent. A mesterséges intelligencia rendszerek megszilárdítására tett lépések növelhetik az általános biztonságot, s a rendeltetésszerű működés biztosítását. Az egyik ilyen lépés az értékelő eszközök bevezetése lenne a telepítés előtt. Ezek az eszközök tesztelik a mesterséges intelligencia-rendszert számos ismert ellenséges módszerrel szemben, annak érdekében, hogy kvantitatív mércét adjanak a robusztusságának (Starck et al., 2022).

A reverse engineering, ami tulajdonképpen egy modellopó támadásnak felel meg, azt a célt szolgálja, hogy az ellenség kinyerje az MI-rendszer által tanultakat, és végül lehetővé tegye a

modell rekonstrukcióját. A támadás végrehajtásához az ellenfélnek képesnek kell lennie arra, hogy bemeneteket küldjön egy modellnek, majd megfigyelje a kimeneteket. Ezzel a támadással megkerüljük magának a modellnek a titkosítását. A támadás során az ellenfél különböző típusú járművek képét küldi és megfigyeli, hogy melyek váltanak ki választ az MI-ből. Ezzel az információval az ellenség képessé válik az MI rendszer másolatának elkészítésére. Amellett, hogy ez a módszer más ellenséges támadások kidolgozását is megkönnyíti, a mesterséges intelligencia döntéseinek közvetlen ismerete lehetővé teszi az ellenfél számára, hogy előre jelezze a válaszokat. Az ilyen jellegű támadás elleni védelem nehéznek bizonyul, és elsősorban a rendszerek megfelelő szabályozása tud valamiféle megoldást jelenteni (Starck et al., 2022).

A gépi tanulás biztonságának érdekében a legfontosabb elem az adatbiztonság. Mivel a gépi tanulási modellek az adatok minőségétől és integritásától függenek, megsértésük, - mint ahogy a támadások esetében is láthattuk - veszélyeztethetik a modell kimeneteit, pontatlan előrejelzésekhez vagy döntésekhez vezetve, amelyek súlyos következményekkel járhatnak. Az adatok a gépi tanulás sarokkövei, így védelmük kulcsfontosságú annak érdekében, hogy az ezen technológiát használó rendszerek kiberbiztonsága is biztosítható legyen. A megfelelő védelem biztosításának érdekében elengedhetetlen a titkosítás. A nyugalmi és átviteli adatok titkosítása biztosítja, hogy azok védve maradjanak a támadásokkal szemben, akár tárolva, akár megosztva. A szigorú hozzáférés-ellenőrzések és hitelesítési mechanizmusok megerősítik a gépi tanulási rendszereket a potenciális kiberfenyegetésekkel szemben. Ezen túlmenően a szerepalapú hozzáférés-vezérlés megvalósítása lehetővé teszi annak pontos kezelését, hogy ki férhet hozzá az adott tudáshoz. Az egyének csak a szerepükhöz és feladatkörükhöz szükséges engedélyekkel rendelkeznek, ezzel korlátozzuk az adatok szükségtelen kitettségét. Hasonlóképpen, a többfaktoros hitelesítés beépítése is egy biztonsági réteget képez azáltal, hogy több ellenőrzési módszerrel ellenőrzi a felhasználói azonosságot. A folyamatos adatellenőrzés és -felügyelet kritikus fontosságú a biztonsági fenyegetések azonosításában és mérséklésében, korai figyelmeztető rendszerként működve a potenciális sebezhetőségekkel vagy támadásokkal szemben. Ez a proaktív megközelítés lehetővé teszi, hogy gyorsan orvosoljuk a biztonsági hiányosságokat. Azáltal, hogy a kezdetektől fogva biztonságot tervezünk, biztosítható ezen modellek rugalmassága, csökkentve a rosszindulatú támadások és adatszivárgások kockázatát (Amos, 2024).

Ezen rendszerek biztonságának megteremtése egyszerre tűnik lehetetlen vállalásnak és kulcsfontosságú, megoldandó problémának. Az viszont egész biztos, a biztonság csak akkor

teremthető meg, ha az ilyen rendszerek esetében az ember mindig a ciklusban marad, s még így is bőven maradnak biztonsági rések.

5.3 Az autonóm fegyverrendszerek kiberbiztonságának megteremtése

Mint ahogy arra az előző fejezet rámutatott, az autonóm fegyverrendszerek számos olyan kiberbiztonsági szempontból aggasztó sérülékenységgel rendelkeznek, melyek kihasználása fatális hibákhoz vezethet, akár gondatlanságból, akár egy kibertámadás következtében.

Az ilyen jellegű technológiák kiberbiztonságának megteremtése kulcsfontosságú. Látnunk kell azt, hogy ezen rendszerek sebezhetőségeinek kihasználása a támadóknak mindig is érdekükben fog állni, hiszen a katonai előnyszerzés eszközeként tekinthetünk rájuk. Az előnyszerzés elérése, attól függően, hogy milyen célt szolgál (a fegyver megsemmisítése, a fegyver feletti kontroll átvétele) nem feltétlenül csak fizikai úton a legkönnyebb, s az ilyen jellegű támadásokat a háború törvényei hivatottak is szabályozni. Mindazonáltal a kibertámadások nehezen visszakövethetőek, mely során relatíve gyorsan és hatékonyan gyengíthető az ellenfél. Minden, aminek van szoftvere az támadható, s nem csak támadható, de támadni is fogják. Abban az esetben ez hatványozottan igaz, amikor adott technológia bőven rendelkezik sebezhetőségekkel, melyek kihasználása az egyik fél számára beláthatatlan következményekkel, míg a másik fél számára előnyszerzéssel jár. Éppen ezért az autonóm fegyverrendszerek kiberbiztonságának megteremtése kulcsfontosságú, melyhez elengedhetetlen a megfelelő szabályozói környezet, annak érdekében, hogy ténylegesen kikényszeríthető legyen. Ez a korábban tárgyalt okok miatt korántsem olyan egyszerű, már csak abból kifolyólag sem, hogy a különböző országok is teljesen különböző szinten állnak ezen fegyverek fejlesztését, valamint a fegyverrendszerek fogalmi meghatározását illetően. Jelenleg nem létezik, s feltételezhetően a közeljövőben nem is fog létezni olyan szabályozás, mely ezen fegyverrendszerek kiberbiztonsági szabályozását nemzetközi szinten kikényszeríti az államoktól.

Nem meglepő módon az Egyesült Államok élen jár az autonóm fegyverrendszerek fejlesztésében és telepítésében. A Védelmi Minisztérium, már 2012-ben kiadta a *DoDI 3000.09, Autonómia a Fegyverrendszerekben (Autonomy in Weapon Systems)* című irányelvét, amely az autonóm és félautonóm fegyverrendszerek fejlesztését és alkalmazását szabályozza. Az irányelvet, 2023-ban ismét frissítették, annak érdekében, hogy ne csak az új rendszerek

fejlesztése és telepítése, hanem a biztonság terén is az élvonalban maradhassanak (Garamone, 2023).

A kiberbiztonság szempontjából jelen direktíva minden rész esetén kiemeli, hogy a *DoDI 8500.01 Kiberbiztonsági irányelvet (Cybersecurity)* kell figyelembe venni, s ennek megfelelően kialakítani a rendszerek biztonságát. Így ennek értelmében ezen direktíva az irányadó a következő kérdésekben:

- rendszerbiztonság, manipuláció elleni mechanizmusok és kiberbiztonság
- az autonóm és félautonóm fegyverrendszerek mesterséges intelligencia képességének és kiberbiztonságának figyelemmel kísérése, de ebben az esetben az *DoDI 3000.09-es Autonómia a Fegyverrendszerekben* irányelv is irányadó, hiszen ez tartalmazza a mesterséges intelligenciára vonatkozó szabályokat
- kibernetikai túlélőképesség, műveleti rugalmasság és kiberbiztonság
- a rendszerbiztonság, a szabotázs elleni mechanizmusok, a kiber reziliencia, az operatív biztonság és a biztonsági rendszerek tervezése során jelen irányelv, továbbá a *DoDI 5000.83-as Technológia és Programvédelem a Technológiai Előny Fenntartása Érdekében (Technology and Program Protection to Maintain Technological Advantage)* irányelve az irányadó

A rendszerbiztonság, a manipuláció elleni mechanizmusok, a kiber reziliencia, a működési rugalmasság és a kiberbiztonsági képességek a *DoDI 5000.83-as irányelv*, a *Közös Képességek Integrációs és Fejlesztési Rendszer Kézikönyve (Joint Capabilities Integration and Development System Manual)* és a *DoDI 8500.01* szerint kerültek bevezetésre a meghibásodások valószínűségének és következményeinek minimalizálása érdekében. Továbbá felügyeleti rendszer van érvényben a működési környezetben, az adatbevitelben és -felhasználásban bekövetkező olyan változások azonosítására és kezelésére, amelyek hozzájárulhatnak a rendszerek meghibásodásához. A *DoDI 5000.89 Tesztelés és Értékelés (Test and Evaluation)* irányelv van érvényben annak ellenőrzésére, hogy a fegyverrendszer ellenálló és túlélőképes-e a kibertérben, vitatott körülmények között (DoD, 2023).

Európai viszonylatban az Egyesült Királyság már fejleszt ilyen fegyverrendszereket, s 2023-ban még nagyobb szerepet kapott a mesterséges intelligencia autonóm rendszerekben való felhasználásának kérdésköre. Annak érdekében, hogy a Lordok Háza minden felmerülő kérdésre választ kapjon, felállításra került a Mesterséges Intelligencia a Fegyverrendszerekben

Bizottság, mely 2023. márciusától novemberig dolgozott azon a közel száz oldalas jelentésen, mely olyan kérdésekre hivatott választ adni, mint az autonóm fegyverrendszerek kockázatai, kihívásai, etikai aggályai, továbbá, a szabályozási lehetőségek, és a humanitárius jog megfeleltetésének a vizsgálata. A vizsgálandó kérdések között bár szerepel, hogy milyen technológiai, jogi, eljárási vagy egyéb biztosítékokra lenne szükség a biztonságos, megbízható és elszámoltatható autonóm fegyverrendszer garantálásához, azonban a jelentés nem vizsgálja mélyrehatóan a kiberbiztonsági lehetőségeket, s a rendszerek fejlesztésében betöltött fontos szerepét (Salerno-Garthwaite, 2023).

A jelentés hivatkozik a 2019-ben Hagyományos Fegyverekről Szóló Egyezmény részes államai által jóváhagyott tizenegy vezérelvre², mely a halálos fegyverek fejlesztésével és használatával kapcsolatos. Ennek megfelelően kiemeli azt az elvet, hogy az ilyen rendszerek jelentős mértékben kitéttek a kibertámadásoknak, s figyelembe kell venni az új fegyverrendszerek kifejlesztésekor vagy beszerzésekor a fizikai biztonságot, valamint a megfelelő kiberbiztonságot, a hackelés vagy az adatok meghamisításának elkerülése érdekében. Ezen kívül a jelentés és egyéb dokumentum nem tárgyalja részletesen az ilyen jellegű rendszerek kiberbiztonságának megteremtésére vonatkozó követelményeket (House of Lords, 2023).

Bár az autonóm fegyverrendszerekkel számos nemzetközi szerv foglalkozik, az egyik legjelentősebbnek a korábban említett ENSZ CCW bizonyul. Az Egyes Hagyományos Fegyverekről szóló Egyezmény (CCW) Magas Szerződő Feleknek 2023-as találkozója úgy határozta, hogy 2024 márciusában és augusztusában megszervezik a Magas Szerződő Felek Kormányzati Szakértői Csoportját a halálos autonóm fegyverrendszerek területén kialakulóban lévő technológiákkal kapcsolatban. Továbbá, a halálos autonóm fegyverrendszerek területén megjelenő új technológiák normatív és működési keretéhez kapcsolódó egyéb lehetőségeket is tárgyalni kívánják (United Nations, 2024). Ebből kifolyólag, feltételezhetően a kiberbiztonság kérdéskörét is szükséges érinteniük, ám eddig erről nem rendelkezünk információval.

Az autonóm fegyverrendszerek kiberbiztonsági szabályozása kulcsfontosságú, azonban meghaladja a szakértők jelenlegi tudását. Az, hogy fontos, abban mindenki egyetért, viszont megfelelő kialakítását illetően számos kérdés merül fel. Amikor az autonóm fegyverrendszerek

² A tilalmakról szóló egyezmény magas szerződő feleinek 2018. évi találkozója az egyes hagyományos fegyverek használatának tilalmáról, korlátozásáról tárgyaltak, melyek túlságosan káros vagy megkülönböztetés nélküli hatásúnak minősülő fegyverek. A kormányszakértők csoportja az újonnan megjelenő technológiákkal kapcsolatban a halálos, autonóm fegyverrendszerek esetében is célúzéseket fogalmazott meg, s tárgyaltak az egyes fegyverek használatának tilalmáról vagy korlátozásáról. Itt fogalmazták meg azt a 11 vezérelvet, mely az autonóm fegyverrendszerek esetében megerősített irányadó elveknek minősülnek (CCW, 2019).

kihívásairól beszélünk, a szakértői csoportok ülésein nem a kiberbiztonság az elsődleges szempont. A jogi, etikai és humanitárius kérdések vannak jelenleg előtérben, s ameddig ezekre nem találunk megfelelő válaszokat, a kiberbiztonság kérdésköre háttérbe szorul.

5.4 Ha a kiberbiztonság megdől – Robotok a bíróság előtt?

Bármilyen magas kiberbiztonságot is sikerül elérni az ilyen autonóm rendszerek esetében, sajnos itt hatványozottan áll fent annak a veszélye, hogy a kiberbiztonság esetlegesen megdől. Mire számíthatunk, s a következményekért ki a felelős? Bíróság elé állítható egy robot? Ebben az esetben két dolgot fontos megvizsgálni. Az autonóm rendszerek meghibásodásából származó károkat, valamint a kibertámadások miatti károkozás kérdéskörét.

A rendszer meghibásodását illetően a legnagyobb probléma a felelősségre vonhatósági űr. Amennyiben az autonóm módon működő rendszer elszabadulva, civil áldozatokat ejt ki a felelős? Mivel az autonóm fegyverrendszert nem lehet jogilag személynek tekinteni, így felelősségre vonni sem lehet. Az operátor, vagy a parancsnok felelősségre vonása pedig nem lenne tisztességes, hiszen a rendszer nem azt csinálta ami az ő szándékában állt. A felelősségre vonhatósági űr, abból is következik, hogy balesetek emberekkel is megesnek, és nem mindig olyan körülmények között, hogy valakit egyértelműen felelősségre lehessen vonni érte. A humanitárius jog egyik alapelve sem mondja ki, hogy a háborúban elkövetett minden halálesetért felelősségre kell vonni valakit, a hadseregek által végrehajtott akciókért végső soron pedig az államok felelősek. A felelősségre vonhatóság nem is azért bír ekkora jelentőséggel, hogy a rendszer meghibásodása esetén valakit meg lehessen büntetni, hanem azért, mert képes elrettentő hatásként funkcionálni. Amennyiben az autonóm fegyvereket bevetők úgy gondolják nem lehet őket felelősségre vonni, könnyen gondatlanná válhatnak és olyan esetekben és környezetben is bevethetik ezen fegyverrendszereket, ahol annak biztonságos működése nem garantálható (Scharre, 2019).

A háború törvényei kimondják, hogy a gépek nem hadviselő felek. A háborúkat emberek vívják és nem robotok. Ez azt is kimondja, hogy ahhoz, hogy egy támadás törvényes legyen szükség van bizonyos emberi közreműködésre. Ennek értelmében a hadviselő feleknek, vagy bármely autonóm fegyvert használó személynek kötelessége a támadás törvényességének biztosítása. Egy ember átruházhatja a specifikus célzási döntéseket egy fegyverre, de nem annak az eldöntését, hogy támadjon-e vagy sem. Ebből is következik, hogy a teljes mértékig autonóm fegyverrendszerek használata törvényellenes, s nem létezik olyan törvény vagy biztonsági

szabályozás, amely képes lenne ezt a problémát kezelni. Az embernek mindig a ciklusban kell maradnia, annak érdekében, hogy a fegyver megfeleljen a háború törvényeinek (Scharre, 2019).

Látható, hogy a fegyverrendszerek üzemeltetéséből fakadó balesetek utáni felelősségre vonás is problémás kérdés, s jelenleg sincsen konszenzus a megoldást illetően. Mi a helyzet abban az esetben, ha egy autonóm fegyverrendszer kibertámadás következtében követ el jogellenes cselekedetet? Ki a felelős ilyenkor és ezt mi hivatott szabályozni? Az ilyen támadások hátterében sok esetben nemzetállamok vagy pedig nem állami szereplők állnak, s ebben az esetben elkövetett támadások esetében már kiberműveletekről beszélhetünk. Ez pedig felvet egy újabb égető problémát, a kiberműveletek szabályozási kérdéseit.

6 AZ AUTONÓM FEGYVERRENDSZEREK ÉS A KIBERFEGYVEREK SZABÁLYOZÁSI KÉRDÉSEI

Nem képezi vita tárgyát, hogy mind az autonóm fegyverek, mind a kiberfegyverek olyan beláthatatlan károk bekövetkezését képesek előidézni, melyek elkerülése érdekében sok esetben még a szabályozói környezet sem elégséges. Éppen ezért, a nemzetek közös érdeke az, hogy minél elkötelezettebben és minél erőteljesebben foglaljanak állást ezen fegyverek szabályozási kérdésiben, legyen szó a fizikai vagy a digitális térről.

Az ilyen és ehhez hasonló technológiákról elmondható, hogy sok ország szándéka nem nyilvánvaló a fejlesztésükkel kapcsolatban. Nyilvánvalóan egyetlen ország sem dicsekszik egy kiberfegyver kifejlesztésével, s az autonóm rendszerek tekintetében elért eredményeiket sem osztják meg a konferenciákon egymással. Több nemzet mellett foglal állást, hogy ezen technológiák fejlesztésére csupán a megfelelő védekezés megteremtése érdekében van szükségük, ám mi a garancia arra, hogy azon fegyvert, mely alapvetően védekezésre lett kifejlesztve, nem használják támadás végrehajtására. Tudomásul kell venni, hogy ezen technológiák jelen vannak, s mint az igaz általánosságban az ilyen és ehhez hasonló technológiákra, szabályozásuk könnyebbnek bizonyul, mint betiltásuk. Éppen ebből kifolyólag is kulcsfontosságú a megfelelő és egységes szabályozói környezet megteremtése, mely sajnos jelenleg még hagy kivetnivalót maga után (Unidir, 2017).

Fontos elsősorban tisztázni azt, hogy bár ezen technológiák inkább tűnhetnek a jövő technológiáinak, mintsem a ma fegyvereinek, azt biztosan tudjuk, hogy mind az autonóm fegyverek mind pedig a kiberfegyverek már jelen vannak, jelentős fenyegetést okozva. Az autonóm fegyvereket és kiberfegyvereket a szabályozás tekintetében, a jobb megértés érdekében bizonyos mértékben érdemes együtt is megvizsgálni, a korábban említett összefüggéseik miatt. Az autonóm kiberfegyverek tulajdonképpen az autonóm fegyverek egy specifikus csoportját alkotják, s a szabályozás tekintetében hasonló nehézségekkel nézünk szembe esetükben.

A probléma alapját mind a két esetben azon hasonlóságok alapozzák meg, hogy mind egy autonóm fegyver mind egy kiberfegyver képes teljes emberi beavatkozás nélkül működni, miközben a rendszer kezelője akár egy másik kontinensen is tartózkodhat. A legnagyobb problémát pedig mind a két esetben az jelenti, hogy ezen fegyverek beláthatatlan károkat képesek okozni, főleg abban az esetben, ha az autonóm fegyver válik egy kiberfegyver célpontjává. A legnagyobb kérdés pedig az, hogy a már meglévő jogi normák képesek-e ezen

kérdésekre választ adni, tudnak-e ezen fegyverek esetében érvényesülni, vagy jelenleg még „törvényen kívül álló” technológiákról beszélünk? Olyan technológiák ezek, melyeket az évtizedekkel ezelőtt létrehozott nemzetközi jog tud egyáltalán értelmezni? A probléma körbejárására a következő kutatási kérdést és hipotézist fogalmaztam meg:

- **Kutatási kérdés 1:** Alkalmas a nemzetközi humanitárius jog arra, hogy szabályozza a kiberműveleteket?
- **Hipotézis 1:** A nemzetközi humanitárius jog önmagában nem elegendő ahhoz, hogy szabályozza a kiberműveleteket, különös tekintettel a kiberfegyverek kérdéskörére.

6.1 Autonóm fegyverek a humanitárius jog alapján - Az új szabályozási rendszer kialakításáért, valamint a betiltásukért vívott harc

Mindaz ismert, a háború törvényeit a nemzetközi humanitárius jog hivatott szabályozni, így nem meglepő módon a szakemberek egy olyan fegyver esetében, mely képes a harctereket átalakítani, elsősorban a már meglévő jogi normákat vizsgálták, s próbálták meg értelmezni az autonóm fegyverrendszerek esetében. Mindazonáltal a nemzetek és a szakértők véleménye korántsem egységes a témában. Vannak, akik a humanitárius jog alkalmazását tartják járható útnak, és vannak, akik egy teljesen új, egységes szerződés létrehozását szorgalmazzák, ám akadnak olyanok is, akik erősen foglalkoznak állást a betiltásuk mellett.

Az autonóm fegyverrendszereket a nemzetközi humanitárius jogról szóló szerződések nem szabályozzák külön, ugyanakkor vitathatatlan, hogy minden autonóm fegyverrendszernek alkalmasnak kell lennie arra, hogy a nemzetközi humanitárius joggal összhangban lehessen csak használni. Mivel a humanitárius jog, szabályokat fogalmaz meg a támadások végrehajtásához szükséges fegyverek használatáról, melyek betartásáért a harcoló felek felelősek, azt mondhatnánk, hogy ezen fegyvereket a humanitárius jognak teljes mértékben képesnek kellene lennie szabályozni (Davison, 2017).

Mindezek ellenére a humanitárius jog hagy kivetnivalót maga után, melyet az Egyesült Nemzetek Szövetségének (ENSZ) évek óta zajló egyeztetései is alátámasztanak. Ugyanis az ENSZ első bizottsága 2023 októberében jóváhagyta a halálos autonóm fegyverekről szóló új határozattervezetet. Az állásfoglalás aggodalmát fejezi ki az autonóm fegyverrendszereknek a globális biztonságra, valamint a regionális és nemzetközi stabilitásra gyakorolt lehetséges negatív következményeivel és hatásaival kapcsolatban, ideértve egy kialakuló fegyverkezési

verseny kockázatát. Kiemeli, hogy a humanitárius jognak érvényesülnie kell az autonóm fegyverrendszerek tekintetében, mindazonáltal az egységes szabályozás érdekében további szerződések szükségesek, hogy ezen fegyverrendszerek esetében ne maradjon szürke zóna a humanitárius jogban (United Nations, 2023).

Bár a nemzetközi humanitárius jog tilt bizonyos fegyvereket, és általános korlátozásokat ír elő az összes többi használatára vonatkozóan is, az autonóm fegyverrendszereket szabályozó külön nemzetközi megállapodás nélkül azonban az államok eltérő álláspontot képviselhetnek ezen általános szabályok alkalmazásáról. Fontos kiemelni, hogy itt a szabályozás erőteljes tiltásokat és korlátozásokat eszközölne. Ezek közé tartozik annak korlátozása, hogy hol, mikor és mennyi ideig használják ezen fegyvereket, milyen típusú célpontokra csapnak le és milyen nagyságrendű erőt alkalmaznak, valamint biztosítják a hatékony emberi felügyelet lehetőségét, továbbá az időben történő beavatkozást és hatástalanítást (United Nations, 2023).

Nyilvánvalóan az egyeztetések a témát illetően nem nyerik el maradéktalanul minden ország tetszését. Volt, aki kiemelte, hogy ezen fegyverrendszerek hatékonyabbak lehetnek, mint egy emberi operátor, és csökkenthetik a hiba lehetőségét, továbbá a nemzetközi jog teljes mértékben vonatkozik ezekre a fegyverrendszerekre (United Nations, 2023).

Mindazonáltal vannak a vitáknak olyan szereplői is, akik úgy gondolják a szabályozás sem állítaná meg ezen fegyverrendszereket attól, hogy rövid időn belül „gyilkos robotok”-ká fejlődjenek. Ha egy autonóm fegyverrendszer a fegyveres erő alkalmazásának tilalmát megsértve mégis fegyveres erőhöz folyamodna akkor megsérti az erőszak alkalmazásának tilalmát, s lényegtelen, hogy amúgy megfelel-e a megkülönböztetés és az emberiség elveinek. Mivel az ilyen fegyvereket működtető rendszerek tanulási funkciója kiismerhetetlen, lehetetlen annak megjósolása, hogy egy robot a jogellenes erőszak alkalmazása mellett fog-e dönteni, nem beszélve arról, hogy a programozás tartalmazhat hibás nézeteket arra vonatkozóan, hogy mikor jogszerű az erőszak alkalmazása (O’Connell, 2023). A betiltásért folytatott harcban további ellenérvként emelik ki, hogy bár a háború törvényei kötik ezen fegyvereket, mégsem képesek a megkülönböztetésre és az arányosság elvének betartására. Amíg többszáz évvel ezelőtt a katonák egyértelműen megkülönböztethetőek voltak, addig napjainkban a modern háborúk színterén sokszor gerillák, egyenruhák és civil ruhák tömkelege keveredik, ahol bizonyos esetekben még az elv sem teljesül, hogy aki rád lő, az ellenség. Így ebből kifolyólag a gép nem tud különbséget tenni katonák és civil között, s a civileket érintő támadások pedig egyértelműen sértik a háború törvényeit. A gép az előre beprogramozott parancsot képes végrehajtani, s bár dönt, de mérlegelni képtelen. A háború káoszában katonák által pillanatok

alatt meghozott döntéseket egy autonóm rendszer képtelen végrehajtani, s ez akaratlanul is baráti és civil áldozatokhoz vezethet. De tovább menve az arányosság elvének betartása is hagy kivetnivalót maga után. Ez az elv kimondja, hogy bármely támadás esetén a katonai szükségszerűségnek nagyobbnak kell lennie, mint a várható civil járulékos veszteségnek. Képes egy gép eldönteni azt, hogy mekkora járulékos veszteség lehet arányos? A gép kezébe lehet adni, annak az eldöntését, hogy egy katonai célpont mellett lévő emberek civilek vagy katonák? És még ha ezt képes is eldönteni, miképpen tudja súlyozni a katonai szükségességet a civil áldozatokkal szemben? Ezen döntések meghozatalához a gépnek emberi szintű morális ítélőképességgel kellene rendelkeznie, mely nem túlzás azt állítani, hogy meghaladja a napjaink technológiáit (Scharre, 2019).

Az autonóm fegyverek szabályozási kérdései nagy port kavarnak, jogosan. Jelenleg még nem lehet teljes bizonyossággal kiemelni, hogy mely megoldás lesz a legcélravezetőbb a szabályozás tekintetében, jelenleg azt tudjuk biztosra mondani, hogy a törekvések zajlanak és szükségesek, s talán nem túlzás azt állítani, hogy sürgetőek is. Az autonóm fegyverek bevetése véleményem szerint nem képezi vita tárgyát azt illetően, hogy szigorú szabályozásra szorul, mindazonáltal a diplomamunka terjedelmi határai miatt jelen fejezet nem tárgyalja az egyes szabályozási lehetőségek melletti és elleni érveket.

6.2 A kiberfegyverek szabályozási kérdései a humanitárius jog alapján

Látható, hogy nehézségekbe ütközünk a fizikai térben is, amikor új fegyverek szabályozására kerül a sor, vajon mire számíthatunk akkor a kibertérben? A kibertérre vonatkozó szabályozási kérdések hosszú évek óta parázs viták tárgyát képezik, s talán még összetettebbnek bizonyulnak, mint az autonóm fegyverek szabályozását érintő kérdések.

Amikor a kiberfegyverek szabályozását vizsgáljuk, a nagy egésztől indulva azt szükséges először szemügyre venni, hogy a kibertér, s a kibernüveletek szabályozása jelenleg, hogy áll. Jelen esetben is kézenfekvő az az elképzelés, hogy a már meglévő jogi normák alkalmazásának kellene az irányadónak lennie. Az államok felelősségére vonatkozó nemzetközi jogot a Nemzetközi Jogi Bizottság (ILC) az államok nemzetközi jogellenes cselekményekért való felelősségéről szóló cikkei, valamint a Tallinn Manual 2.0. is vizsgálja, annak érdekében, hogy meghatározza az államok felelősségére vonatkozó szabályok hogyan érvényesülhetnek a kibertérben. Bár az utóbb említett dokumentum semmilyen jogi kötőerővel nem bír, mégis kidolgozott egy olyan szabályrendszert, melyet érdemes figyelembe venni, amikor a

kibertérben zajló műveletekről való szabályozásról beszélünk. Az állam felelősségére vonatkozó jog olyan másodlagos szabályokból áll, amelyek meghatározzák, hogy milyen körülmények között felelős egy állam egy nemzetközileg jogellenes cselekményért. Ez azt jelenti, hogy egy olyan magatartásnak (lehet ez cselekedet vagy mulasztás) kell fennállnia adott ország részéről, mely a nemzetközi jog valamely elsődleges szabályának a megsértését jelenti egy másik államnak fennálló kötelezettségével szemben. A kiberkontextusban ez azt jelenti, hogy a nemzetközi jogellenes cselekmény olyan kiberművelet, amely sérti a nemzetközi jog valamely elsődleges szabályát, s ezért kerül górcső alá. A Stuxnet, mint autonóm kiberfegyver esetében is úgy ítélték meg, hogy jogellenes cselekményt követtek el, s ez az eset tökéletes példa arra is, amikor egy kibertámadás fizikai kárt is okozott. Az autonómia a kibertérben is tovább árnyalja a szituációt, hiszen az autonóm rendszerekkel kapcsolatban gyakran felmerülő kérdés a vétkesség vagy szándékosság kérdésköre, valamint az, hogy a rendszer autonómiája hogyan és milyen mértékben képes befolyásolni a felelősség kérdéskörét, itt is felmerül (Liivoja & Väljataga, 2021).

Az említett példa is összetettnek bizonyul, ám csak egy szeletét emeltem ki a problémának, mely az autonómia kérdésköre. A legnagyobb probléma a szabályozás terén továbbá, hogy nem létezik egységes, mindenki által elfogadott fogalom a kiberfegyverre, mint olyanra. Ez határozott problémát vet fel a szabályozás tekintetében, hiszen nehezen lehetséges jogi keretek kialakítása valami olyan jelenségre, aminek nincsen egységes értelmezése.

A kiberfegyverek szabályozásának nehézsége abban is gyökerezik, hogy soha azelőtt ilyen problémával még nem találkoztunk, így nehéz más területről „kölcsön venni” szabályozási mintákat. Kézenfekvő példa a nukleáris fegyverek esete. Amíg a nukleáris fegyverzetellenőrzés központi pillérei, mint például a nukleáris fegyverek elterjedésének megakadályozásáról szóló szerződés, a stratégiai fegyverzetcsökkentéssel kapcsolatos szerződés folyamata és a 2017-es nukleáris fegyverek betiltása csak korlátozottan valósulhatnak meg a kibertérben. Az átláthatóság nyilvánvalóan szintén problémát okoz a szabályozás tekintetében. Amíg az atomfegyverek, vagy egyéb fegyverek sok esetben számszerűsíthetőek, szembetűnőek, addig a kiberfegyverek megfoghatatlanok és titkosak, mely által ellenőrzésük szinte lehetetlenné válik. Nehéz megismerni, hogy kinek milyen kiberfegyver van a birtokában, ezáltal nehéz meghatározni, hogy mit is kellene szabályozni. A másik jelentős nehézség a felelősségi kör meghatározása. A fizikai térben használt fegyverek esetében - mely költségek és erőforrások szempontjából is jelentősnek bizonyulnak – az államok vannak a főszerepben, s a felelősség is őket terheli. Ám a kibertérben, ahol sok esetben meghatározhatatlan, hogy mely állam vetette

be az adott kiberfegyvert (egyáltalán állami szereplővel állunk-e szemben), kifejezetten nehézé válik a felelősség meghatározása (Futter, 2020).

6.2.1 Tallinn Manual 2.0 – Érvényesülhetne a nemzetközi jog a kibertérben?

Jelenleg az egyetlen kézzel fogható dokumentumként azt illetően, hogy a kiberműveletek esetében a nemzetközi jog miképpen érvényesülne a Tallinn Manuel első és második kiadása szolgál. A Tallinn Manual 2.0 az első részt bővíti ki, és 154 "black letter" szabályt határoz meg a kiberműveletekre vonatkozóan. Bár a Tallinn Manual 2.0 az Európai Bizottság álláspontját és szakértők személyes véleményét képviseli, továbbá hozzájárult számos állam is, jelen dokumentum jogi kötőerővel nem bír, inkább ajánlasként, iránymutatásként szolgál (CCDCOE, 2024).

Érdemes megvizsgálni a Tallinn Manual 2.0 vonatkozó részét azt illetően, hogy mit fogalmaz meg a kiberfegyverek esetében. A Genfi egyezmények I. kiegészítő jegyzőkönyvének 36. cikke rendelkezik az „Új fegyverekről”, melynek célja, hogy minden új fegyvert, eszközt vagy módszert felül kell vizsgálni annak biztosítása érdekében, hogy azok megfeleljenek a nemzetközi humanitárius jognak. A 36. cikk szerint ennek a felülvizsgálatnak meg kell határoznia, hogy alkalmazásuk "bizonyos vagy minden körülmények között" tilos-e (ICRC, 2023).

Ezen szabály teljesülését a kibertérben, így a kiberfegyverekre vonatkozóan a Tallinn Manual 2.0 110-es szabálya tenné lehetővé. A felesleges sérülésekre, a szükségtelen szenvedésre és a válogatás nélküli fegyverekre vonatkozó tilalmak alapján logikusan következik, hogy valamilyen felülvizsgálatot kell végezni annak megállapítására, hogy egy kiberfegyver sérti-e vagy sértheti-e ezeket a tilalmakat. Ennek érdekében a Tallinn Manual úgy rendelkezik, hogy minden állam köteles biztosítani, hogy az általa beszerzett vagy használt kiberhadviselési eszközök megfeleljenek a fegyveres konfliktusok jogának őket kötelező szabályainak. Továbbá az I. kiegészítő jegyzőkönyv részes államai kötelesek a kiberhadviselés új eszközének vagy módszerének tanulmányozása, fejlesztése, megszerzése vagy elfogadása során meghatározni, hogy annak alkalmazása bizonyos vagy valamennyi körülmény között tilos lenne-e az említett jegyzőkönyv vagy a nemzetközi jog rájuk vonatkozó bármely más szabálya alapján (Schmitt, 2017).

És ezen kikötésekkel együtt, jelenleg ez minden, amit a kiberfegyverek humanitárius jognak való lehetséges megfeleléséről és szabályozásáról tudunk, nem beszélve az autonóm kiberfegyverek problematikájáról.

6.2.2 Új egyezmény vagy a nemzetközi jog alkalmazása a kiberfegyverek szabályozása érdekében?

A fent említettek fényében jogosan merül fel a kérdés, hogy ez elégséges lehet-e? Az elmúlt években több vita tárgyát is képezte az az elgondolás, hogy a nemzetközi jog alkalmazható a kibertérben, s ezzel együtt a kibernüveletekre is, így a már meglévő jogi normákat kellene értelmezni. Jelen fejezetben szeretném bemutatni, hogy miért ütközhet akadályokba a nemzetközi jog alkalmazása, s a nagy egésztől indulva először a nemzetközi jog és a kibertér problematikáját megvizsgálva jutunk el ahhoz a kérdéskörhöz, hogy miért lenne szükség a kiberfegyverek szabályozásának érdekében egy új egyezményre.

A nemzetközi jog a technológia tekintetében kiterjed minden olyan eszközre, amelyet az államok és a nem állami szereplők egyaránt használnak. Következésképpen nem kétséges, hogy a nemzetközi jog alkalmazható az internetre és más digitális információs és kommunikációs technológiákra egyaránt, átfogva azok múltbeli, jelenlegi és jövőbeli fejlődését is (Akanke et al. 2022). Mindazonáltal a nemzetközi jog hatékonyságát illetően, problémákba ütközünk, amikor például a végrehajtási mechanizmus hiányát említjük. A nemzeti joggal ellentétben, amelyet a nemzeti bíróság hajt végre, a nemzetközi jognak nincs központi hatósága vagy mechanizmusa a betartásának biztosítására. Következésképpen megnehezíti az államok felelősségre vonását a nemzetközi jog normáinak megsértéséért. A nemzetközi jog a támogatás hiánya miatt is problémásnak tekinthető. A nagyhatalmak könnyen úgy dönthetnek, hogy figyelmen kívül hagyják vagy megsértik a nemzetközi jogot, ha az ellentétes nemzeti érdekeikkel vagy külpolitikai céljaikkal. Vegyünk csak egy példát: az Egyesült Államok hosszú múltra tekint vissza a nemzetközi jog, köztük az Egyesült Nemzetek Alapokmányának figyelmen kívül hagyásában vagy megsértésében. Az Egyesült Államok az ENSZ Biztonsági Tanácsában vétőjogát is felhasználta már arra, hogy megakadályozza a nemzetközi jog érvényesítését. A nemzetközi jog támogatottsága azért is alacsony, mert az gyakran nem egyezik a nagyhatalmak érdekeivel. Nézzük meg, hogy a nemzetközi jog nem terjed ki a kémkedésre, mert bár senki sem akarja, hogy kémkedjenek utána, mindenki szeretne információkat szerezni más országokról (Advocate, 2023).

Ezek a problémák önmagukban is megnehezítik a nemzetközi jog alkalmazását, nem beszélve arról, ha alkalmazását a kibertérre próbáljuk kivetíteni. A kiberháborúk, a kibertámadások teljesen más jellegűek, mint a hagyományos értelemben vett támadások. A kibertérben a nemzetközi jogban tárgyalt elrettentés nem alkalmazható. Míg a nemzetközi jog szerint a potenciális támadókat elrettenthetik tetteik súlyos következményei vagy költségei, a kibertér egyik jellemzője éppen az, hogy az elrettentés szinte nem létezik. Az erőszakos cselekmények természetüknél fogva rejtve maradnak, ezért a kibertérben nem lehet, vagy kifejezetten nehéz felelősségre vonni az elkövetőket. Míg a kibereseményeknek egyértelmű végpontjai vannak, ahol a támadás észlelhető, a kiindulópont gyakran nem egyértelmű és könnyen elrejthető. Míg egy rakéta esetében a röppálya és a műszaki adatok alapján ellenőrizhető, hogy honnan lőtték ki, addig egy kiberbotnet általában nem rendelkezik ezekkel az információkkal. Arról nem is beszélve, hogy egy ország megvádolása is félresikerülhet, ha a támadó kiléte nem teljesen bizonyos (Mártonffy et al. 2022).

Sajnos el kell ismerni, hogy a nemzetközi jogban jelentős hiányosságok vannak a kibertérben való alkalmazás tekintetében. Éppen ezek a hiányosságok mutatnak rá egy új szerződés szükségességére. A szerződés megkötésére irányuló erőfeszítések már elég régóta folynak. Gondoljunk csak az ENSZ kormányzati szakértői csoportjainak 2010 óta tartó üléseire, vagy az ENSZ által 2017-ben létrehozott nyílt munkacsoportra. A többoldalú koordináció és normakövetés terén figyelemre méltó kezdeményezés volt a kibertér stabilitásával foglalkozó globális bizottság, amelyet 2019-ben hoztak létre. Szintén 2019 novemberében indította el a francia kormány a Párizsi Felhívást a kibertér bizalmáért és biztonságáért, amelynek egyik fő támogatója a Microsoft volt. Aláírói (több mint ezer különböző kormányzati és magánszervezet, tudományos és szakmai szervezet) kilenc önkéntes szabványt írtak alá. Az alapelvek a korábbi, többoldalú tárgyalások eredményeire épülnek (Mártonffy et al. 2022).

A kiberműveletek és azon belül is a kiberfegyverek szabályozási kérdései, bőven túlmutatnak a jelenlegi ismereteinken. Az viszont talán kijelenthető, hogy egy ennyire komplex és új kérdéseket felvető témakörben a nemzetközi jog, s azon belüli humanitárius jog önmagában aligha lenne képes egyértelmű válaszokat adni. Mindazonáltal látni kell azt, hogy a meglévő humanitárius jog is csak a fegyveres konfliktusokra vonatkozik, nem terjed ki a belső feszültségekre vagy zavargásokra, például az elszigetelt erőszakos cselekményekre, valamint, csak akkor alkalmazandó, ha a konfliktus már elkezdődött, és akkor is egyformán vonatkozik minden félre, függetlenül attól, hogy ki kezdte a harcot. A szerződés nem a fegyverfejlesztés és a kiberháború elleni küzdelem tekintetében merül fel, hiszen ez szinte elkerülhetetlen. Jelen

esetben is az az érv érvényesülne, hogy amit megtiltani nem tudunk azt legalább szabályozni próbáljuk meg. A felelősség kérdésköre itt a legnehezebb, s pont úgy, mint az autonóm fegyverek esetében, jelenleg is az egyik legnehezebb kihívást jelentik a szabályozás terén (Eilstrup-Sangiovanni, 2017).

Úgy gondolom jól látható, hogy valami hiányzik a nemzetközi humanitárius jogból, és ezért nem lehet a kibertérben úgy alkalmazni, ahogyan kellene. A nemzetközi humanitárius jog jó alap lenne, és merem állítani, hogy a kibernüveletek és kiberfegyverek szabályozása is része lehetne ennek, de a kiberképességek hihetetlen fejlődési üteme miatt ezen jog alkalmazása szinte lehetetlen. Ez alátámasztja a felállított hipotézist, ami alapján a nemzetközi humanitárius jog önmagában nem elegendő ahhoz, hogy szabályozza a kibernüveleteket, különös tekintettel a kiberfegyverek kérdéskörére.

A legnagyobb probléma azonban véleményem szerint az, hogy beszélhetünk nemzetközi jogról vagy szerződésekről, de amíg ezek nem kikényszeríthetőek, addig felesleges köröket futunk. Akár nemzetközi jognak, akár szerződésnek nevezzük, az államok érdekei mindent felülírnak. Egy biztos, a szabályrendszert most kell kidolgozni. Elmondhatjuk, hogy itt az ideje, hiszen ezen kiberképességek már régóta jelen vannak, mindazonáltal nem lesz könnyű dolga a szakembereknek, hiszen a kibertérben felhasználható képességek esete ugyanaz, mint a kémkedés... mindenki használni akarja ezeket a kiberképességeket, de senki sem akarja, hogy ellene használják őket.

7 EMPIRIKUS VIZSGÁLAT

7.1 Módszertan és hipotézis

Mint az a dolgozatban említésre került, az autonóm fegyverrendszerek és a kiberfegyverek a modern háború részét képezik. Annak érdekében, hogy mérni tudjuk azt, hogy egy autonóm képességekkel rendelkező dróntámadásnak³, vagy kiberműveletnek milyen hatása volt, váltott-e ki egyáltalán hatást, az eseményelemzés módszertant fogom használni. Az eseményelemzés, avagy az event study módszer elsősorban arra a kérdésre ad választ, hogy *Számít-e az adott esemény?* hiszen méri egy adott esemény azonnali és rövid távú késleltetett hatását az értékpapír értékére. A módszer nem csak a közgazdaságtan, de napjainkban akár a jog és a politika területén is egyre nagyobb teret kap (W. Brandt M, 2010).

A módszer használata során meg kell határoznunk a vizsgálni kívánt eseményt, azt, hogy ez az esemény mikor következett be, mely során kulcsfontosságú, hogy olyan időpontot vegyünk alapul, mely esetében feltételezhetjük, hogy a piac ténylegesen tudomást szerzett az eseményről (Pandey & Kumari, 2021) (Gáll & Lublőy, 2012). A módszer vázát tulajdonképpen az képezi, hogy egy adott felállított hipotézist a bekövetkezett események és az általuk kiváltott hatásokon keresztül vizsgál.

Ahhoz, hogy a módszertant elvégezzük, egy megfigyelési időszakot veszünk alapul. Vizsgáljuk az esemény előtti időszakot, mely jelen esetben 35 napot fed le, valamint vizsgálatra kerül az esemény utáni 3 nap annak érdekében, hogy mérni tudjuk, hogy megfigyelhető-e abnormális hozam, tehát volt-e hatása az eseménynek.

A módszertan szabad kezet ad ezen időintervallumok meghatározása esetében, viszont célszerű figyelembe venni azt, hogy maga a helyzet, amiben vizsgálódunk mennyire turbulens. A 35 nap valójában 10 és 25 napra oszlik. A 10 nap az eseményt közvetlenül megelőző időszak, ami során az abnormális hozamot mérjük, míg a 25 nap az eseményt megelőző 11. naptól méri a normális hozamot, majd egymáshoz is hasonlítjuk őket, hogy minél pontosabb eredményt kaphassunk. Figyelembe véve az esetleges egyéb támadásokat (amik megelőzték vagy éppen követték a kiválasztott eseményeket) a 35 nap képes kisimítani a hozamokban fellelhető esetleges kiugró értékeket, melyek a háború eredményeként elég gyakorinak tekinthetők a

³ Mivel nincsen információnk azt illetően, hogy bizonyos országok milyen fejlettségi szintű autonóm fegyverrendszerekkel rendelkeznek, így az elemzés szempontjából releváns, autonóm képességekkel rendelkező drónok kerülnek vizsgálatra.

turbulens időszaknak köszönhetően. Azonban ez a 35 nap mégsem bizonyul túl hosszú időintervallumnak, szintén figyelembe véve, hogy háborúról beszélünk (Wolf et al., 2014).

A normális hozam megállapítása a háború fényében kifejezetten nehéznek bizonyul, hiszen egy ilyen időszak turbulens, az események egymást követik, viszont a jelen megfigyelési időszak lehetővé teszi, hogy megállapítsuk, hogy a háború fényében mi nevezhető normális hozamnak. A hatások érvényesülésének vizsgálata érdekében az eseményt követő 3 nap is a vizsgálati időszak részét képezi, (ez nem része a korábban említett 35 napnak) ez az eseményablak, ahol választ kapunk arra a kérdésre, hogy megfigyelhető-e abnormális hozam. Ez a normális hozamtól való eltérést jelenti, amely által megállapítható, hogy az eseménynek volt-e hatása (Pandey & Kumari, 2021) (Gáll & Lublóy, 2012). A 3 nap szintén az egyéb támadások figyelembevételével került kiválasztásra. A 3 nap alatt kimutathatók késleltetett hatások is, mindazonáltal nem tudunk a piac által is ismert egyéb jelentős támadásról, amely befolyásolná az eredményeket.

Milyen adatokat kellett meghatározni?	Mit vizsgáltam?	A meghatározott adatok
Események és az események időpontja	Esemény hatásának a vizsgálata	A kiválasztott 3 dróntámadás és a 2 kibertámadás
Eseményablak	Részvények változásának vizsgálata az esemény hatására	3 nap
Megfigyelési időszak	Normális hozam és abnormális hozam mértékének a vizsgálata	35 nap

1.táblázat: A módszertanban alkalmazott adatok ismertetése (Forrás: saját szerkesztés)

A felállított kutatási kérdés és hipotézis, melyet az ismertetett módszertannal vizsgáltam pedig a következő:

- **Kutatási kérdés 2:** Képesek-e befolyásolni az autonóm képességekkel rendelkező drónok által elkövetett támadások, valamint a kiberműveletek a tőzsde alakulását, hatást gyakorolnak-e a piacra, ezen események?
- **Hipotézis 2:** Az autonóm képességekkel rendelkező drónok általi támadások és kiberműveletek nem feltétlenül befolyásolják a piacot és nem minden esetben okoznak változást a részvények árfolyamában.

7.2 Adatok ismertetése

Az elemzés során összesen öt esemény, három dróntámadás és két kibertámadás vizsgálatára került sor. Három jelentős dróntámadás hatását vizsgáltam a moszkvai MOEX Tőzsdére, a Ukrenergo ukrán villamos-energia átvitelért felelős vállalat részvényeire, valamint a Northrop Grumman amerikai dróngyártó cég részvényeire. Az Ukrenergo részvényeinek vizsgálatára azért került sor, mert elsősorban az energia szektort ért támadásokat vizsgáltam, a Northrop Grumman vállalat részvényei esetében a fő fókusz azon volt, hogy egy-egy dróntámadás után figyelhető-e meg emelkedés a részvényeik esetében, a moszkvai MOEX tőzsdének pedig jelentős a kitettsége a jelenlegi időszakban. Annak érdekében, hogy az esetleges hatások minél jobban bizonyíthatóak legyenek, az Ukrán Tőzsdét is szerettem volna vizsgálni, mindazonáltal az ukrán jegybank a háború óta rögzítette az árfolyamot, így nem lehetséges az események vizsgálata ezen tőzsde esetében (Harmash, 2023).

A három vizsgált esemény kiválasztásánál a fő szempont az volt, hogy olyan dróntámadások legyenek, melyek az energetikai szektort érték vagy érintették, ismerten autonóm képességekkel rendelkező drónokkal követték el, és a támadás napján nem volt tudomásunk, a piac által is ismert kibertámadásról, valamint egyéb nagyobb volumenű fizikai támadásról. Ennek okán a következő események hatása került vizsgálatra:

1. 2022. december 10-én Oroszország iráni gyártmányú Shaded-136 drónokat használt két energialejesztmény eltalálására, így 1,5 millió ember maradt áram nélkül több régióban (Starkov, 2022).
2. 2023. február 11-én Oroszország újabb csapást mért Ukrajna amúgyis megtépázott villamos energia-hálózatára, szintén iráni Shaded-136 drónok használatával (Vinograd, 2023).

3. 2023. december 29-én Oroszország az egyik legnagyobb légitámadást indította Ukrajna ellen inváziója kezdete óta, példátlan számú drón és rakéta bevetésével (Vogt et. al., 2023).

Esemény megnevezése	Rövidítés	Esemény dátuma
Oroszország iráni gyártmányú drónokat használt két energialejesztmény eltalálására, így 1,5 millió ember maradt áram nélkül több régióban.	DRÓN_1	2022. december 10.
2023. február 11-én Oroszország újabb csapást mért Ukrajna amúgyis megtépázott villamos energia-hálózatára, szintén iráni Shaded-136 drónok használatával.	DRÓN_2	2023. február 11.
2023. december 29-én Oroszország egyik legnagyobb légitámadást indította Ukrajna ellen teljes körű inváziója kezdete óta, példátlan számú drón és rakéta bevetésével.	DRÓN_3	2023. december 29.

2.táblázat: A vizsgált dróntámadások jellemzőinek összegző táblázata (Forrás: saját szerkesztés)

Az eseményeket a jelentősebb nemzetközi hírközlési portálokon lévő hírek alapján választottam ki, s egyeztettem a támadás, a hír megjelenésének idejét, valamint a tőzsde nyitásának időpontját. Mivel 2022. december 10. és 2023. február 11. szombatra esett, 2023. december 29. pedig péntekre - tekintve, hogy hétfőgén nem jegyzi a tőzsde az adatokat - így az elemzés során, azt az időpontot vettem alapul, amikor a tőzsde erről tudomást szerzett, mely a támadásokat követő hétfő.

A kibertámadások esetében két eseményt vizsgáltam abból kifolyólag, hogy olyan volumenű kibertámadásra volt szükség a vizsgálat érdekében, amikor is más esetlegesen nagyobb hatást kiváltható fizikai támadás nem történt, vagy ha mégis, a hírportálok akkor is a kibertámadást emelték ki. Bár történt több, jelentősnek mondható kibertámadás is, az érintett vállalatok nem érhetőek el a tőzsdén. A kibertámadások esetében egyedi hatást mértem, azt vizsgáltam, hogy

az adott vállalatokra nézve volt-e hatása az őket ért kibertámadásnak. Így ebben az esetben a Viasat KA-SAT és a VEON⁴ részvényei kerültek vizsgálatra.

A két vizsgált kibertámadás a következő:

1. 2022. február 24-én, az orosz inváziót megelőző órákban kibertámadás indult a Viasat KA-SAT szatellit hálózata ellen, mely jelentős zavarokat okozott Európa szerte (Vasquez & Groll, 2023).
2. 2023. december 12-én Ukrajna egyik legnagyobb mobilhálózat-szolgáltatóját, a Kyivstart érte kibertámadás, melynek következtében Ukrajna lakosságának több, mint fele mobil-szolgáltatás nélkül maradt napokra. A támadás megrongálta az informatikai infrastruktúrát, és emberek millióit veszélyeztette, hogy nem kapnak riasztást az esetleges légítámadásokról, mivel Kijev egyes részein magát a légriadó rendszert is megzavarta (Hunder et al., 2023).

Esemény megnevezése	Esemény rövidítése	Esemény dátuma
A Viasat KA-SAT szatellit hálózata elleni kibertámadás, mely jelentős zavarokat okozott Európa szerte.	TÁMADÁS_1	2022. február 24.
Ukrajna egyik legnagyobb mobilhálózat-szolgáltatóját, a Kyivstart érte kibertámadás, mely több jelentős kárt is okozott országszerte.	TÁMADÁS_2	2023. december 12.

3.táblázat: A vizsgált kibertámadások jellemzőinek összegző táblázata (Forrás: saját szerkesztés)

7.3 Elemzés és eredmények

Az egyes tőzsdei adatok esetében az események által gyakorolt abnormális hozamok eredményeit tartalmazza az alábbi táblázat. Az események szignifikanciája 5% alatt számít, ebben az esetben mondható el, hogy az eseménynek volt hatása (a magas százalék nem tükrözi az esemény jelentőségét, csupán azt mutatja meg, hogy volt-e hatása az események) (Wolf et al., 2014).

⁴ Bár a támadás a Kyivstart érte, a vállalat nem érhető el a tőzsdén, így az anyavállalat, a VEON került vizsgálatra, aki szintén reagált a kibertámadásra és tájékoztatta az érintetteket az incidenskezelés során (VEON, 2023).

	Tőzsde	Abnormális hozam (%)	t-statisztika (szám)	Szignifikancia (%)
DRÓN_1	Northrop Grumman	1,4%	0,54	59,50%
	Ukrenergo	-2,39%	-0,77	44,75%
	Moszkvai Tőzsde	-0,55%	-0,49	62,53%
DRÓN_2	Northrop Grumman	0,83%	0,46	64,75%
	Ukrenergo	-7,19%	-1,07	29,68%
	Moszkvai Tőzsde	-0,01%	-0,01	99,37%
DRÓN_3	Northrop Grumman	0,38%	0,38	70,88%
	Ukrenergo	-1,40%	-1,56	13,08%
	Moszkvai Tőzsde	0,18%	0,26	79,56%

4.táblázat: A dróntámadások hatásainak ismertetése (Forrás: saját szerkesztés)

Az elemzés során megállapítható, hogy egyik esemény vonatkozásban sincsen szignifikáns hatás, hiszen a szignifikancia minden esetben 5% feletti. A vizsgált eredmények tekintetében nem értelmezhető abnormális hozam az eseményből fakadóan, mely azt jelenti, hogy az esemény nem váltott ki jelentős, számszerűen mérhető változást, így az események nem befolyásolták a részvények alakulását.

Ez többek között, köszönhető annak, hogy az orosz-ukrán háború kitörése hatással volt a világ tőzsdéire és az azóta is megfigyelhető turbulens időszakra a piacok folyamatosan reagálnak, az árazások tükrözhetik a támadásokra való felkészülést. Ebből kifolyólag egy támadás már nem „üt” akkorát a piac tekintetében. A piac felkészülhet arra, hogy a modern háborúban drónokat vetnek be, és maga a drón bevetése nem feltétlenül éri el az ingerküszöböt. Ez arra utal, hogy a drónok, mint autonóm képességekkel rendelkező fegyverek, részévé válnak a modern háborúknak, és nem érik el azokat az ingerszinteket, amelyek korábban meghatározták a konfliktusok hatásait. Emellett pedig a piac ingerküszöbének kitolásában az is meghatározó tényező, hogy a dróntámadások után megjelenő reakciók és válaszok kiemelik, hogy hány drónt sikerült megsemmisítenie a légvédelemnek, hangsúlyozva azt, hogy felkészültek ezen

támadásokra, így a reakciók is jelentős mértékben alakítják a piac hozzáállását ezen támadásokhoz.

A kibertámadások esetében a következő eredmények születtek:

	Tőzsde	Abnormális hozam (%)	t-statisztika (szám)	Szignifikancia (%)
TÁMADÁS_1	Viasat	2,77%	1,01	32,24%
TÁMADÁS_2	VEON	0,23%	0,09	92,85%

5.táblázat: A kibertámadások hatásainak ismertetése (Forrás: saját szerkesztés)

A kibertámadások jellegükből fakadóan nehezebben mérhetőek, és kevesebb információ is áll rendelkezésünkre ahhoz, hogy több esemény, akár esemény sorozat hatását vizsgáljuk. A kiberműveletek sok esetben csak később, hónapok, vagy akár évek múlva derülnek ki, így nem minden esetben lehetséges a piacra gyakorolt hatásukat valós időben mérni. Ezen két esemény esetében elmondható, hogy nem volt jelentős hatás megfigyelhető, nem gyakoroltak hatást az események a vállalatok részvényeire.

A VIASAT esetében ez köszönhető annak is, hogy a kiberműveletet követően pár órával megkezdődött az offenzíva Ukrajna ellen, mely akár képes volt önmagában nagyobb hatást kiváltani. A Kyivstar esetében, a VEON anyavállalat reakciójából ítélve elmondható az is, hogy nem érte őket teljesen váratlanul a támadás, kijelentették, hogy a kibertérben is zajlik a háború, melynek ők is áldozatává váltak, amely ebben a környezetben könnyen megtörténhet, dolgoznak a minél gyorsabb incidenskezelésen (Hunder, 2023).

Egy háború során nem újkeletű, sőt szinte egyértelmű, hogy a kritikus infrastruktúrák nem csak a fizikai térben, de a kibertérben is fő célpontokká válnak, melyekre nem csak a vállalatoknak, a piacnak is fel kell készülnie. Ez úgy gondolom ebben az esetben is látható, hiszen az, hogy a támadás nem váltott ki jelentős hatást, köszönhető a háború turbulens időszakának, valamint annak, hogy egy háborúban elkövetett kibertámadás a piac ingerküszöbét nem feltétlenül éri el. Továbbá, Ukrajna az elmúlt években kifejezetten kitett volt a kibertámadásoknak. Itt elsősorban nem is azon van a hangsúly, hogy ezen támadások mennyire voltak sikeresek, inkább azon, hogy éberren tartották a piaci szereplőket, hiszen számoltak az esetleges támadásokkal (Mueller,

2023). Ezen támadások beépülhetnek a piac árazásába, mintegy felkészülésként a későbbi támadásokra. Továbbá, Oroszország a fizikai térben is jelentős pusztítást végzett bizonyos kritikus infrastruktúrák esetében, így egy lebombázott szektor ellen elkövetett támadások a hatékonyság hiánya miatt nem feltétlenül érik el a piac ingerküszöbét.

Azzal, hogy a vizsgált események nem váltottak ki hatást, a felállított hipotézis elfogadásra került, így elmondható, hogy az autonóm képességekkel rendelkező drónok általi támadások és kiberműveletek nem feltétlenül befolyásolják a piacot és nem mindig okoznak változást a részvények árfolyamában.

8 ÖSSZEGZÉS

Az a mértékű technológiai fejlődés, amely az elmúlt években megfigyelhető volt, jelentősen érzékeltette hatását a katonai szektorban is. A mesterséges intelligencia katonai felhasználása, nem csak számos új lehetőséget, de kihívást és veszélyt is teremtett. A „gyorsabban, magasabbra, erősebben” elv pedig arra ösztönzi a világ vezető hatalmait, hogy olyan mértékben fejlesszék és alkalmazzák a mesterséges intelligenciát, amely képes minden harctéri szerepet és feladatot megváltoztatni. Ezt tükrözik az autonóm fegyverrendszerek fejlesztésére tett törekvések is. Bár az autonóm fegyverrendszerek inkább tűnnek a jövő technológiájának, mintsem a ma fegyverének, nem tudunk elmenni a tény mellett, hogy nem rendelkezünk elegendő információval azt illetően, hogy az országok hogyan is állnak ezen rendszerek fejlesztésével, amely aggályokat vet fel. Az elmondható, hogy zajlik a munka a fejlesztésüket illetően, így elérkezett annak az ideje, hogy számoljunk velük, felkészüljünk rájuk és képesek legyünk elkerülni a jövő „robokálipszist”.

A téma rendkívül összetett és olyan fogalmi koncepciók hiányoznak, melyek nem csak az autonóm fegyverrendszerek kérdéskörének megértését nehezítik, de egyéb problémát is felvetnek. Az autonóm rendszerek jogi, etikai és kiberbiztonsági kihívást is jelentenek, s bár amíg a szabályozásra tett törekvések esetében a viták zajlanak, a kiberbiztonság jelenleg még háttérbe szorul. Mindazonáltal ezen rendszerek esetében a kiberbiztonság kulcsfontosságú, hiszen minden ilyen jellegű rendszer támadható, s könnyen kibertámadás célpontjává válhat. Ez pedig egy újabb kérdéses területet nyit meg, a kibernműveletek szabályozásnak fontosságát.

Vita tárgyát képezi, hogy a nemzetközi humanitárius jog, képes-e szabályozni a kibernműveleteket. A nemzetközi humanitárius jog alkalmazhatósága bár nemzetközi megítélések szerint működőképes lehet, sajnos sok esetben nem bizonyul elégségesnek a kibernműveletek, különös tekintettel a kiberfegyverek esetében. A kiberháborúk és kibertámadások teljesen más jellegűek, mint a hagyományos értelemben vett támadások. A kibertérben a nemzetközi jogban tárgyalt elrettentés nem alkalmazható. Míg a nemzetközi jog szerint a potenciális támadókat elrettenthetik tetteik súlyos következményei vagy költségei, a kibertér egyik jellemzője éppen az, hogy az elrettentés szinte nem létezik. Az erőszakos cselekmények természetüknél fogva rejtve maradnak, ezért a kibertérben nem lehet, vagy kifejezetten nehéz felelősségre vonni az elkövetőket, mely problémákra a humanitárius jog jelenleg nem képes megoldással szolgálni. Mindezek alapján megállapítom, hogy a H1-es hipotézisem megerősítésre került. A vizsgálataim alapján megállapítottam, hogy a nemzetközi

humanitárius jog önmagában nem elegendő ahhoz, hogy szabályozza a kiberműveleteket, különös tekintettel a kiberfegyverek kérdéskörét.

Az esemény elemzés módszertannak köszönhetően, látható, hogy az autonóm képességekkel rendelkező drónok és a kiberműveletek nem minden esetben hatnak a piacra. Ezen módszertan segítségével megállapítottam, hogy ezek a támadások nem minden esetben érik el a piac ingerküszöbét. Ezzel a H2-es hipotézisem megerősítésre került, miszerint az autonóm képességekkel rendelkező drónok általi támadások és kiberműveletek nem befolyásolják a piacot és nem okoznak szignifikáns változást a részvények árfolyamában.

Elmondható, hogy ezen új technológiák a modern háborúk részévé válnak, és a jövőben ennél már csak nagyobb törekvést figyelhetünk majd meg a még fejlettebb és még szofisztikáltabb támadások végrehajtására, mind a fizikai, mind pedig a kibertérben. Éppen ebből kifolyólag elengedhetetlen, hogy nagy hangsúlyt fektessünk, mind a jogi mind pedig a kiberbiztonsági kérdésekre, hiszen ezek már nem a jövő technológiái, hanem a ma fegyverei.

Diplomamunkám során rengeteg érdekes és figyelemfelkeltő kérdésbe ütköztem, minél mélyebbre ástam, annál szerte ágazóbb területeket figyeltem meg, melyek újabb kutatási területeket tárnának fel számomra. Úgy gondolom az autonóm fegyverrendszerek kérdésköre, az autonóm képességekkel rendelkező drónok általi támadások hatásai átfogóbban is vizsgálhatók egyéb területek bevonásával. A kibertámadások hatásainak vizsgálata pedig szintén további kutatási kérdéseket vet fel, a kiberműveletek és kiberfegyverek szabályozási lehetőséginek vizsgálatával együtt.

9 Irodalomjegyzék

Könyvek, folyóirat cikkek:

1. Akande, D., Coco, A., & Souza Dias, T. (2022). *Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies*. International Law Studies
2. Billig, C. D., Fordy G., Friedl, K. E, Hasselstrom H. (2020). *The implications of emerging technology on military human performance research priorities*, Journal of Science and Medicine in Sport 24 (2021) 947-953. DOI: 10.1016/j.jsams.2020.10.007
3. Chavannes, E., & Arkhipov-Goyal, A. (2021). *The Ethics of Robotic and Autonomous Systems in a Military Context*, Hague Centre for Strategic Studies, pp. 51-115.
4. Futter, A., (2020). *What does cyber arms control look like? Four principles for managing cyber risk*, Global Security Policy Brief, London, Creative Commons Attribution-ShareAlike 4.0.
5. Davison, N., (2017). *A legal perspective: Autonomous weapon systems under international humanitarian law*, UNODA Occasional Papers No. 30, November 2017, pp 5-18, DOI: <https://doi.org/10.18356/29a571ba-en>
6. Eilstrup-Sangiovanni, M., (2017). *Why the World Needs an International Cyberwar Convention*, Philos. Technol. (2018) 31:379–407, DOI 10.1007/s13347-017-0271-5
7. Gáll I. & Lublőy Á. (2012): *A jelzálogpiaci válság és a Közép-Kelet-Európában aktív nagybankok részvényárfolyama*. Hitelintézeti Szemle, 11.évf. 3.sz., pp. 185-210
8. Liivoja, R., Väljataga, A., (2021). *Autonomous Cyber Capabilities under International Law*, Tallinn, NATO CCDCOE Publications
9. Madan, B., B., Banik, M., Bein, D. (2016). *Securing unmanned autonomous systems from cyber threats*, Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 2019, Vol. 16(2) 119–136, DOI: 10.1177/1548512916628335
10. Mártonffy, B., et al. (2022). *Kiberdiplomácia*, Ludovika Egyetemi Kiadó.
11. Munk, S. (2018). *A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései*, Hadtudomány 2018/1, DOI 10.17047/HADTUD.2018.28.1.113
12. O’Connell, M. E., (2023). *Banning Autonomous Weapons: A Legal and Ethical Mandate*. Ethics & International Affairs. 2023;37(3):287-298. doi:10.1017/S0892679423000357

13. Pandey, D. K. & Kumari V. (2021): *Event study on the reaction of the developed and emerging stock markets to the 2019-nCoV outbreak*. International Review of Economics and Finance, 71. pp. 467-483.
14. Perez, L. (2023). *Is Stuxnet the next Skynet? Autonomous cyber capabilities as lethal autonomous weapons systems*, Artificial Intelligence and International Conflict in Cyberspace, 1. kiadás, Routledge
15. Scharre, P., (2019). *A terminátor eljövetele*, 1.kiadás, New York: W.W. Norton&Company
16. Schmitt, M. N., (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press
17. Unidir (2017). *The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations*, No. 7

Jogi dokumentumok, szabályozók, ajánlások:

18. DoD, (2023). *DOD DIRECTIVE 3000.09 - AUTONOMY IN WEAPON SYSTEMS*, Office of the Under Secretary of Defense for Policy, 2023. január 25, Forrás: <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>
letöltés dátuma: 2024. március 21.
19. United Nations, (2024). *Convention on Certain Conventional Weapons — Group of Governmental Experts on Lethal Autonomous Weapons Systems Overview*, United Nations Office for Disarmament Affairs, Forrás: <https://meetings.unoda.org/ccw-/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2024> letöltés dátuma: 2024. március 23.
20. CCW, (2019). *Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects*, Final Report, Geneva, 13–15 November 2019.
21. House of Lords (2023). *Proceed with Caution: Artificial Intelligence in Weapon Systems*, AI in Weapon Systems Committee, Report of Session 2023–24.
22. ICRC (2023). Article 36 - *New weapons*, International Humanitarian Law Databases, <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-36> letöltés dátuma: 2024. február 10.

Internetes források:

23. Advocate, Q. M. Q., (2023) *International Law: Challenges and Limitations to Effectiveness*, The Law Studies, Forrás: <https://www.thelawstudies.org/2023/01/Why-international-law-ineffective-challenges.html> letöltés dátuma: 2023. november 19.
24. Amos, Z., (2024). *How to Secure Machine Learning Data*, Global Cybersecurity Alliance, Forrás: <https://gca.isa.org/blog/how-to-secure-machine-learning-data> letöltés dátuma: 2024. március 23.
25. Ari, B. (2023). *Autonomous Cyber Weapons*, LinkedIn, Forrás: <https://www.linkedin.com/pulse/autonomous-cyber-weapons-ari-basen-cissp> letöltés dátuma: 2023. november 19.
26. Boston Dynamics (2023), *About - FAQs ABOUT BOSTON DYNAMICS*, Forrás: <https://www.bostondynamics.com/about#Q7> letöltés dátuma: 2024. január 4.
27. CCDCOE, (2024). *International Law Applies to Cyber Operations, Tallinn Manual 2.0 Reaffirms*, CCDCOE, Forrás: <https://ccdcoe.org/news/2017/international-law-applies-to-cyber-operations-tallinn-manual-2-0-reaffirms/> letöltés dátuma: 2024. április 9.
28. Eliaçık, E. (2022). *Guns and Codes: The era of AI-wars begins*, Dataconomy, Augusztus 17. Forrás: <https://dataconomy.com/2022/08/how-is-artificial-intelligence-used-in-the-military/> letöltés dátuma: 2023. október 24.
29. Garamone, J., (2023). *DOD Updates Autonomy in Weapons System Directive*, U.S. Department of Defense, Forrás: <https://www.defense.gov/News/News-Stories/Article/Article/3278065/dod-updates-autonomy-in-weapons-system-directive/> letöltés dátuma: 2024. március 20.
30. Harmash, O. (2023). *Ukraine eases fixed exchange rate for first time during war*, Reuters, Forrás: <https://www.reuters.com/markets/currencies/ukraines-central-bank-introduces-managed-flexibility-exchange-rate-2023-10-02/> letöltés dátuma: 2024. április 2.
31. Hunder, M., Landay, J., Bern, S., (2023). *Ukraine's top mobile operator hit by biggest cyberattack of war*, Forrás: <https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers-massive-hacker-attack-statement-2023-12-12/> letöltés dátuma: 2024. április 4.
32. ICRC, (2022). *What we need to know about autonomous weapons*, International Committee of the Red Cross, Forrás: <https://www.icrc.org/en/document/what-you-need-know-about-autonomous-weapons> letöltés dátuma: 2024. március 10.

33. Keller, J., (2021). *Pentagon to spend \$874 million on artificial intelligence (AI) and machine learning technologies next year*, *Military + Aerospace Electronics*, Forrás: <https://www.militaryaerospace.com/computers/article/14204595/artificial-intelligence-ai-dod-budget-machine-learning> letöltés dátuma: 2024. február 23.
34. Lewis, S. (2023). *OODA loop*, *TechTarget*, Forrás: <https://www.techtarget.com/searchcio/definition/OODA-loop> letöltés dátuma: 2023. december 16.
35. LinkedIn (2024). *How do you protect Machine Learning from attacks?*, LinkedIn, Forrás: <https://www.linkedin.com/advice/1/how-do-you-protect-machine-learning-from-attacks> letöltés dátuma: 2024. március 19.
36. LinkedIn, (2023). *Understanding the Risks of AI in Military Applications*, LinkedIn, Forrás: <https://www.linkedin.com/pulse/understanding-risks-ai-military-applications-ai-news> letöltés dátuma: 2024. március 20.
37. Malyasov, D., (2024) *Ukrainian soldiers captured Russian spy drone using robotic vehicle*, *Defence Blog*, Forrás: <https://defence-blog.com/ukrainian-soldiers-captured-russian-spy-drone-using-robotic-vehicle/> letöltés dátuma: 2024. március 20.
38. Miralis D. (2023). *Cyber weapons definition*, *Ngm*, Forrás: <https://ngm.com.au/cyber-weapons-definitions/> letöltés dátuma: 2023. december 11.
39. Mueller, B. G., Jensen, B., Valeriano, B., Maness C., R., Macias M., J., (2023). *Cyber Operations during the Russo-Ukrainian War*, Forrás: <https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war> letöltés dátuma: 2024. április 9.
40. Salerno-Garthwaite, A., (2023). *Lethal autonomous weapons inquiry launched by House of Lords*, *Airforce Technology*, Forrás: <https://www.airforce-technology.com/features/lethal-autonomous-weapons-inquiry-launched-by-house-of-lords/> letöltés dátuma: 2024. március 22.
41. Sheldon, R., (2023). *What are autonomous systems and how do they work?*, *TechTarget*, <https://www.techtarget.com/searchnetworking/definition/autonomous-system> letöltés dátuma: 2023. december 1.
42. Starck, N., Bierbrauer, D., Maxwell, P., (2022). *ARTIFICIAL INTELLIGENCE, REAL RISKS: UNDERSTANDING—AND MITIGATING—VULNERABILITIES IN THE MILITARY USE OF AI*, *Modern War Institute*, Forrás: <https://mwi.westpoint.edu/artificial-intelligence-real-risks-understanding-and-mitigating-vulnerabilities-in-the-military-use-of-ai/> letöltés dátuma: 2024. március 22.

43. Starkov, Nick (2022). *Russia drones smash power network in Odesa*, Forrás: <https://www.reuters.com/world/europe/russian-drone-attacks-target-power-network-ukraines-odesa-officials-2022-12-10/> letöltés dátuma: 2024. április 1.
44. StartUs, (2023). *Top 10 Military Technology Trends & Innovations for 2024*, StartsUs Research Blog, Forrás: <https://www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022/> letöltés dátuma: 2023. november 24.
45. United Nations (2023). *First Committee Approves New Resolution on Lethal Autonomous Weapons, as Speaker Warns 'An Algorithm Must Not Be in Full Control of Decisions Involving Killing'*, United Nations, Forrás: <https://press.un.org/en/2023/gadis3731.doc.htm> letöltés dátuma: 2024. február 13.
46. United Nations (2023). *UN and Red Cross call for restrictions on autonomous weapon systems to protect humanity*, United Nations, Forrás: <https://news.un.org/en/story/2023/10/1141922> , letöltés dátuma: 2024. február 16.
47. Vasquez, C., Groll, E., (2023). *Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault*, CyberScoop, <https://cyberscoop.com/viasat-ka-sat-hack-black-hat/> letöltés dátuma: 2024. április 5.
48. VEON, (2023). *Kyivstar Network Targeted by Widespread Cyber Attack*, VEON, <https://www.veon.com/newsroom/press-releases/kyivstar-network-targeted-by-widespread-cyber-attack> letöltés dátuma: 2024. április 5.
49. Vinograd, C., (2023). *Ukraine Rushes to Repair After Wave of Russian Strikes*, The New York Times. Forrás: <https://www.nytimes.com/2023/02/11/world/europe/russia-ukraine-drone-strikes.html> letöltés dátuma: 2024. április 3.
50. Vogt, A., Sangal, A., Meyer, M., Powell, T. B., (2023). *Russia launches largest air attack on Ukraine since full-scale invasion*, CNN, Forrás: <https://edition.cnn.com/world/live-news/russia-ukraine-war-12-29-23/index.html> letöltés dátuma: 2024. április 4.
51. W., Brandt M. (2010) *Pages from fin econometrics brandt_2*. Slideshare., Forrás: <https://www.slideshare.net/slideshow/pages-from-fin-econometrics-brandt2/4929691> letöltés dátuma: 2024. április 3.
52. Wolf, M. Schimmer, M., Levchenko, A., and Müller, S. (2014). *EventStudyTools (Research Apps)*, St.Gallen. Forrás: <http://www.eventstudytools.com> letöltés dátuma: 2024. április 9.