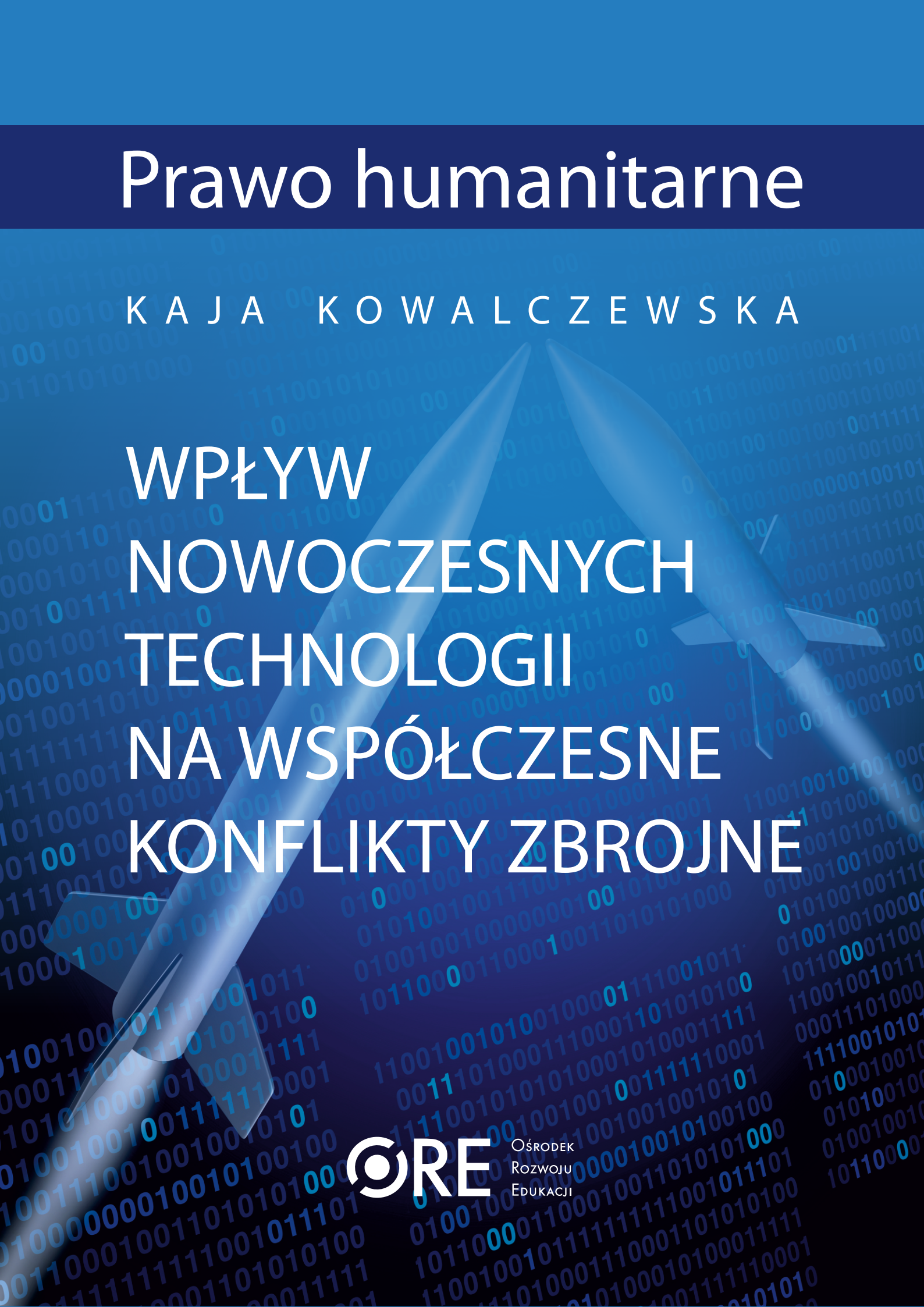
Prawo humanitarne

KAJA KOWALCZEWSKA

WPŁYW NOWOCZESNYCH TECHNOLOGII NA WSPÓŁCZESNE KONFLIKTY ZBROJNE



ORE Ośrodek Rozwoju Edukacji

Prawo humanitarne

K a j a K o w a l c z e w s k a

WPŁYW NOWOCZESNYCH TECHNOLOGII NA WSPÓŁCZESNE KONFLIKTY ZBROJNE

Ośrodek Rozwoju Edukacji
Warszawa 2022

Konsultacja merytoryczna
Wydział Rozwoju Kompetencji Kluczowych
Anna Kasperska-Gochna

Redakcja i korekta
Tomasz Karpowicz

Projekt okładki, layout,
redakcja techniczna i skład
Barbara Jechalska

Fotografia na okładce: © lightsource/Photogenica

Ośrodek Rozwoju Edukacji
Warszawa 2022
Wydanie I

ISBN 978-83-66830-49-3

Publikacja jest rozpowszechniana na zasadach licencji
Creative Commons Uznanie Autorstwa – Użycie Niekomercyjne (CC BY-NC)

00-478 Warszawa
Aleje Ujazdowskie 28
www.ore.edu.pl

Spis treści

Wprowadzenie

TEMATY

A. Międzynarodowe prawo humanitarne a wybrane środki walki
B. Nowe technologie wojskowe:
   - cyberataki
   - sztuczna inteligencja
   - doskonalenie żołnierzy.

GRUPA DOCELOWA

Uczniowie szkół ponadpodstawowych

CELE

- Zrozumienie podstawowych pojęć związanych ze środkami i metodami walki w międzynarodowym prawie humanitarnym
- Poznanie charakterystyk nowych technologii wojskowych
- Zrozumienie konsekwencji użycia nowych technologii wojskowych dla podstawowych zasad międzynarodowego prawa humanitarnego i dla godności ludzkiej

ŚRODKI DYDAKTYCZNE

- Do realizacji zajęć nie potrzebujemy licznych środków dydaktycznych. Zazwyczaj są to materiały wydrukowane lub przesłane uczniom do odczytania na urządzeniach elektronicznych (komputer, laptop, smartfon) oraz tablica.
- Niekiedy trzeba będzie zapewnić połączenie z internetem oraz ekran do wyświetlenia materiałów.

METODY

Podstawowymi metodami proponowanymi w niniejszym materiale są:

- **Dyskusja**: jednym z celów dyskusji jest zachęcanie uczniów do równego udziału. Dobra dyskusja wymaga, by nauczyciel stał się słuchaczem i swoistym twórcą, który zbiera opinie poszczególnych uczniów i układa je w spójną całość. Docelowo to uczniowie powinni stać się takimi twórcami.
- **Burza mózgów**: jej celem jest zachęcenie do samodzielnego myślenia poprzez tworzenie atmosfery tzw. zawieszonego osądu. Umożliwia uczniom tworzenie dowolnej liczby pomysłów w określonym czasie. Jeśli celem jest rozwiązanie problemu, burza mózgów pozwala poszczególnym osobom zgłaszać liczne rozwiązania. Uczniowie mogą następnie podsumować informacje, które zebrali, i przedstawić odpowiedź całej grupy.

- **Wykorzystanie historii**: angażuje umysł i serce. Ta metoda wykorzystuje jedną z najstarszych technik propagowania kultury – opowiadanie historii. W wielu kulturach historie dotyczą zazwyczaj decyzji etycznych, mają wprowadzić uczniów w autentyczne sytuacje i zainicjować dyskusję.
- **Praca w małych grupach**: pomaga uczniom dzielić się poglądami i rozwijać umiejętności. Osobom pracującym na bazie materiałów zaleca się wykonywanie ćwiczeń właśnie w tej formie. Te same grupy mogą wykonywać serię ćwiczeń lub skład grupy może się zmieniać zależnie od zestawu ćwiczeń.

Temat A. Międzynarodowe prawo humanitarne a wybrane środki walki

1. Podstawowe zasady MPH

Nauczyciel przedstawia uczniom podstawowe pojęcia z zakresu międzynarodowego prawa humanitarnego (MPH), zebrane w poniższym słowniczku.

- **Obiekt cywilny** – każdy obiekt, który nie jest celem wojskowym. Jeżeli obiekty cywilne są wykorzystywane do działań militarnych, stają się celami wojskowymi i tracą status obiektów chronionych (jeśli zachodzą wątpliwości co do statusu danego obiektu, tj. nie wiadomo, czy jest on wykorzystywany do wspierania działań zbrojnych, powinien on zostać uznany za obiekt cywilny).
- **Cel wojskowy** – obiekt, który z powodu swej natury, rozmieszczenia, przeznaczenia lub wykorzystania wnosi istotny wkład do działalności wojskowej i którego zniszczenie daje określoną korzyść wojskową.
- **Zasada proporcjonalności** – zabrania się przeprowadzania ataków, co do których można przypuszczać, że spowodują one niezamierzone straty wśród ludności cywilnej i szkody w dobrach cywilnych, łącznie nadmierne w porównaniu z oczekiwaną konkretną i bezpośrednią korzyścią wojskową.
- **Zasada rozróżniania** – strony konfliktu planujące lub przeprowadzające atak powinny zawsze odróżniać ludność cywilną od walczących, a także obiekty o charakterze cywilnym od celów wojskowych.
- **Zakaz powodowania nadmiernego cierpienia lub niepotrzebnego okrucieństwa** – celem prowadzenia działań bojowych jest nie całkowite zniszczenie przeciwnika (np. zabicie wszystkich walczących), ale zmuszenie go poddania się, np. przez pozbawienie go woli do walki; takie osłabienie sił zbrojnych, które nie pozwoli im kontynuować walki (walczący staną się *hors de combat*).
- ***Hors de combat*** – dosłownie znaczy 'wyłączeni z walki': pojęcie opisujące walczących, którzy zostali wzięci do niewoli, są ranni, chorzy lub wyczerpani i z tego względu nie mogą dalej prowadzić walki.
- **Broń „nierozróżniająca"** – uniemożliwiająca rozróżnienie obiektów cywilnych i celów wojskowych: nie sposób jej skierować na określony cel wojskowy, lub nie możliwe jest zapanowanie nad skutkami jej działania.
- **Broń powodująca „niepotrzebne cierpienie"** – broń zadająca walczącym nadmierne cierpienie (np. większe niż potrzebne do powstrzymania ich od walki).

- **Środek walki** – broń lub system uzbrojenia wykorzystywane do przeprowadzenia ataku, skutkującego śmiercią lub obrażeniami, np. strzała, pocisk, system przeciwlotniczy.
- **Metoda walki** – sposób wykorzystania środka walki np. bombardowanie, selektywna eliminacja, metoda spalonej ziemi.

2. Zakazane środki walki

Nauczyciel dzieli uczniów na małe grupy i każdej z nich przekazuje do opracowania jeden ze środków walki opisanych poniżej. Prosi o dokładne zapoznanie się i ewentualnie o wyszukanie dodatkowych informacji w internecie na temat podobnych środków walki. Następnie uczniowie prezentują każdy ze środków walki poprzez podanie odpowiedzi na następujące pytania:

1. Na czym polega sposób działania tego rodzaju broni?
2. Czy istnieją umowy międzynarodowe zabraniające używania tych środków walki?
3. Czy używanie tego rodzaju broni może naruszać jedną lub więcej podstawowych zasad MPH? Jeżeli tak, to które i dlaczego?
4. Czy słyszeliście o użyciu tego rodzaju broni w dotychczasowych konfliktach zbrojnych?

Temat B. Nowe technologie wojskowe

1. Cyberataki i ich skutki

Trudno wyobrazić sobie funkcjonowanie współczesnego świata bez dostępu do internetu i do cyberprzestrzeni. Mówi się wręcz o zjawisku cyfryzacji ludzkiego życia. To zjawisko wpływa również na sposób prowadzenia konfliktów zbrojnych. Świadczy o tym chociażby tworzenie dowództw wojsk zajmujących się cyberprzestrzenią (np. w Chinach, Polsce, Rosji czy Stanach Zjednoczonych).

Uczniom warto przedstawić poniższe statystyki:

- liczba mieszkańców na świecie wynosi ponad 7 mld, ponad 2 mld z nich korzysta z internetu,
- na świecie jest aktywnych ponad 5 mld numerów telefonów komórkowych,
- liczba użytkowników internetu w Polsce wynosi około 24 mln,
- statystyczny użytkownik internetu spędza w sieci 16 godzin miesięcznie, co w skali światowej daje około 35 mld godzin w ciągu miesiąca (czyli w przybliżeniu 4 tysiące lat online na każdy miesiąc kalendarzowy),
- wartość sprzedaży online w USA w pierwszym kwartale 2012 r. osiągnęła 50 mld dolarów,
- wyszukiwarka Google otrzymuje dziennie ponad miliard pytań,
- liczba kont na portalu Facebook przekracza miliard, w tym ponad 10 mln to konta użytkowników z Polski,
- co sekundę w serwisie Youtube pojawia się kolejna godzina materiału filmowego,
- każdego dnia w grze Farmville (wchodzącej w skład portalu Facebook) sprzedaje się około 500 tys. traktorów. W realnym świecie firma John Deere sprzedaje 5 tys. maszyn rolniczych rocznie.

Na podstawie: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" vol. 5(9), 2013, s. 225.

Poproś uczniów o zastanowienie się nad sposobami, w jakie można wykorzystać cyberprzestrzeń, aby zaszkodzić bezpieczeństwu państwa.

Możliwe pytania:

1. Czy atak z wykorzystaniem sieci komputerowej może spowodować skutki w świecie poza siecią komputerową?
2. Czy cyberataki mogą być szkodliwe w takim samym stopniu jak ataki z wykorzystaniem broni konwencjonalnej?
3. Jakie sfery działalności państwa są najbardziej narażone na cyberataki?

Słowniczek:

- **Cyberprzestrzeń** – wirtualna przestrzeń stworzona z sieci cyfrowych, wykorzystywana do przechowywania, modyfikowania oraz przekazywania informacji. Jej częścią jest internet, ale zawierają się w niej także inne systemy informacyjne: obsługujące biznes, infrastrukturę oraz wspomagające świadczenie usług. Sieci cyfrowe już dziś podbudowują proces zaopatrywania domów w energię elektryczną oraz wodę, pomagają organizować dostawy żywności oraz innych dóbr do sklepów oraz służą jako niezbędne narzędzie biznesowe. Ich zasięg ustawicznie się powiększa, w miarę jak podłączamy do nich nasze telewizory, konsole do gier, czy nawet urządzenia AGD.
- **Computer Network Attacks** (CNA, ataki w sieci komputerowej) – działania mające na celu zakłócanie, negowanie, psucie lub niszczenie informacji znajdujących się w komputerach i sieciach komputerowych (lub samych komputerów i tych sieci).
- **Computer Network Exploitation** (CNE, wykorzystanie sieci komputerowej) – zdolność do uzyskania dostępu do informacji przechowywanych w systemach informatycznych oraz możliwość korzystania z samego systemu.
- **Infrastruktura krytyczna** – systemy (rzeczywiste i cybernetyczne) oraz obiekty wchodzące w ich skład i powiązane funkcjonalnie (np. budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania administracji publicznej), a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy:
    a. zaopatrzenia w energię, surowce energetyczne i paliwa,
    b. łączności,
    c. sieci teleinformatycznych,
    d. finansowe,
    e. zaopatrzenia w żywność,
    f. zaopatrzenia w wodę,
    g. ochrony zdrowia,
    h. transportowe,
    i. ratownicze,
    j. zapewniające ciągłość działania administracji publicznej,
    k. produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym – rurociągi substancji niebezpiecznych.

2. Cyberataki to nie science fiction

Nauczyciel dzieli uczniów na trzy grupy. Każdej z nich rozdaje jeden zestaw materiałów o cyberatakach, które miały miejsce i były szeroko omawiane przez specjalistów. Poszukajcie wspólnie odpowiedzi na następujące pytania:

- Czy cyberataki przeprowadzono w związku z trwającym konfliktem zbrojnym? W jakich okolicznościach miały miejsce?
- Na czym polegał cyberatak i jakie były jego skutki?
- Czy udało się ustalić sprawców?

Po przedstawieniu wszystkich historii przeprowadza się burzę mózgów z uwzględnieniem poniższych pytań:

- Dlaczego stosowanie cyberataków można uznać za mniej dotkliwą formę ataku niż atak kinetyczny, np. z użyciem karabinu?
- Na czym polega najpoważniejsza trudność związana z pociągnięciem sprawców do odpowiedzialności?
- Jakie rozwiązania wdrożono, aby zapobiegać takim atakom w przyszłości?

Materiały:

1. Cyberatak na Estonię w 2007 roku
2. Cyberatak na Gruzję podczas wojny z Rosją w 2008 roku
3. Stuxnet i cyberwojna między USA a Iranem

3. Sztuczna inteligencja

Nauczyciel zapoznaje klasę z nagraniem wypowiedzi Petera Singera w formule TED, które znajduje się na stronie www.ted.com/talks/p_w_singer_military_robots_and_the_future_of_war (dostępne są napisy w języku polskim).

Następnie przeprowadza dyskusję w klasie na temat potencjalnych zagrożeń i korzyści z używania robotów podczas konfliktów zbrojnych.

Warto razem rozważyć następujące kwestie:

- Jak jest różnica między dronami bojowymi a systemami uzbrojenia opartymi na sztucznej inteligencji?
- Jakie są wady i zalety zdalnych działań zbrojnych lub działań zbrojnych prowadzonych przez maszyny?
- Czy są jakieś działania, w których systemy oparte na sztucznej inteligencji okazują się lepsze od ludzi?
- Czy podejmowanie decyzji o ataku przez sztuczną inteligencję mogłoby zastąpić proces decyzyjny przeprowadzany przez człowieka?
- Kto powinien ponosić odpowiedzialność za błędy maszyn?

Słowniczek:

- **Sztuczna inteligencja** – obecnie wyróżnia się trzy określenia sztucznej inteligencji porównujące jej zdolności z ludzkimi:
  - wąska sztuczna inteligencja, rozumiana jako algorytmy mające na celu rozwiązanie jakiegoś konkretnego zadania;
  - ogólna sztuczna inteligencja, mająca zdolności intelektualne człowieka (jeszcze nie istnieje);
  - sztuczna superinteligencja, przewyższająca zdolności intelektualne człowieka (również nie istnieje).

- **Sofizmat androida** – zjawisko ufania maszynom w sposób nieuzasadniony i przesadny (zwłaszcza tym humanoidalnym), połączonego ze zrzeczeniem się zasadniczego wpływu na proces decyzyjny.
- **Drony bojowe** – bezzałogowe platformy (powietrzne, morskie, lądowe), sterowane na odległość. Zazwyczaj wykorzystywane do misji zwiadowczych (pozyskiwania danych) lub bojowych (przeprowadzania ataków na cele wojskowe).

4. Doskonalenie żołnierzy

„Człowiek jest najsłabszym ogniwem systemów obronnych (…) nie chodzi o to, by po prostu zastąpić ludzi maszynami, ale by połączyć ludzi z robotami w celu stworzenia bardziej sprawnych, zwinnych i opłacalnych sił, które obniżą ryzyko ofiar w USA".

DARPA (Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności),
Stany Zjednoczone

Nauczyciel prosi uczniów o wymienienie słabych stron człowieka jako żołnierza (tych, które negatywnie wpływają na potencjał wojskowy, np. zmęczenie, konieczność snu i jedzenia, trudności w widzeniu w nocy, zdolność do noszenia tylko ograniczonych ciężarów). Następnie prosi uczniów o dopisanie pomysłów, dzięki którym można wyeliminować te cechy (np. użycie pewnych substancji chemicznych czy wzmocnień fizycznych).

Kiedy uczniowie już przedstawią swoje pomysły, nauczyciel prezentuje klasie rzeczywiste projekty i eksperymenty, które są obecnie stosowane lub nad którymi pracuje się w wojskowych laboratoriach.

Warto przeprowadzić wspólną burzę mózgów, z uwzględnieniem następujących zagadnień:

- Czy daleko posunięte modyfikacje ludzi mogą zagrozić ich godności?
- Czy żołnierze powinni poddawać się tym modyfikacjom dobrowolnie, czy też w tym przypadku interes państwa (publiczny – bezpieczeństwo) jest nadrzędny, a sama modyfikacja powinna być obowiązkowa?
- Jakie mogą być długofalowe konsekwencje takich eksperymentów?

Materiały dla uczniów

1. Zakazane środki walki

Na podstawie: M. Żeligowski, *Zakazy i ograniczenia użycia środków prowadzenia działań zbrojnych w świetle międzynarodowego prawa humanitarnego konfliktów zbrojnych,* [w:] *Międzynarodowe prawo humanitarne konfliktów zbrojnych*, red. Z. Falkowski, M. Marcinko, Wojskowe Centrum Edukacji Obywatelskiej, Warszawa 2014.

Broń chemiczna

Bojowy środek trujący to każdy toksyczny środek chemiczny, który przez swoje działanie na procesy życiowe może spowodować śmierć, czasowe obezwładnienie albo trwałą szkodę na zdrowiu u ludzi lub zwierząt. Ta definicja obejmuje wszystkie związki chemiczne, niezależnie od stanu skupienia, pochodzenia czy metody produkcji.

Tradycyjnie bojowe środki trujące dzieli się na pięć grup:

- środki duszące – substancje chemiczne powodujące upośledzenie procesu przenoszenia tlenu do organów wewnętrznych i – w konsekwencji – ich obumieranie; do takich środków zalicza się cyjanowodór, tlenek węgla, a także cyklon B, stosowany w komorach gazowych w czasie II wojny światowej,
- środki parzące – substancje chemiczne mające postać gęstych, oleistych cieczy rozpylanych w postaci aerozoli i wykazujące działanie trujące zarówno poprzez kontakt ze skórą (powodują trudno gojące się oparzenia), jak i wskutek wdychania oparów uszkadzających drogi oddechowe; do tej grupy należą przede wszystkim iperyty i luizyty,
- środki krztuszące – substancje chemiczne wywołujące u rażonej nimi osoby silny kaszel i obrzęk płuc prowadzący do śmierci; do tej grupy zalicza się chlor i fosgen,
- środki paralityczno-drgawkowe – najbardziej niebezpieczne bojowe środki trujące (śmiertelna dawka niektórych z nich może wynosić nawet 200 mikrogramów); oddziałują bezpośrednio na układ nerwowy: powodują drgawki, porażenie mięśni, a następnie – zatrzymanie akcji oddechowej; te środki to m.in. sarin, VX, soman, tabun i VG,
- psychotoksyczne środki trujące – bojowe środki trujące ukierunkowane nie tyle na pozbawienie życia żołnierzy przeciwnika, ile na doprowadzenie ich do takiego stanu psychicznego, w którym nie zdołają oni prowadzić działań bojowych: doświadczają halucynacji, omamów, tracą orientację w czasie i przestrzeni; do tej grupy należą LSD oraz BZ.

Broń biologiczna

Broń biologiczna to rodzaj broni masowego rażenia, w której czynnikiem rażenia są organizmy żywe o charakterze patogennym, wywołujące różnego rodzaju choroby u ludzi i zwierząt mających styczność z tymi organizmami. Broń biologiczną tradycyjnie dzieli się na trzy grupy:

- wirusy – skomplikowane cząsteczki organiczne łączące cechy organizmów żywych i materii nieożywionej; do wirusów, które były przechowywane jako komponenty broni bakteriologicznej, można zaliczyć przede wszystkim wirus ospy prawdziwej;
- bakterie – obszerna grupa mikroorganizmów, najczęściej o budowie jednokomórkowej; jako czynnik rażenia wykorzystywano pałeczki dżumy i tularemii, a przede wszystkim – laseczki wąglika,
- toksyny – organiczne trucizny wytwarzane przez drobnoustroje, rośliny i zwierzęta; przykłady to botulina (jad kiełbasiany), rycyna i alkaloidy.

Broń nuklearna

Ogromna ilość energii wyzwalana w czasie eksplozji jądrowej w postaci fali uderzeniowej, promieniowania cieplnego i promieniowania przenikliwego prowadzi do porażenia osób i obiektów na obszarze od kilkunastu do nawet 100 kilometrów. Kolejnym, pośrednim, czynnikiem rażenia broni jądrowej jest opad promieniotwórczy, prowadzący do skażenia terenu, mogący się utrzymywać – zależnie od użytych materiałów – od kilku dni do wielu lat i powodować poważne, i długotrwałe szkody środowiska naturalnego. Dopóki aktywność promieniotwórcza nie zmniejszy się do poziomu bezpiecznego dla istot żywych, skażonego terenu nie mogą zamieszkiwać ani wykorzystywać ludzie, a występująca na nim fauna i flora ginie bądź ulega różnego rodzaju mutacjom.

Broń kasetowa

Jest to środek walki, którego działanie opiera się na umieszczeniu w nosicielu (w pocisku rakietowym, bombie lotniczej, granacie moździerzowym czy innym pocisku artyleryjskim, a także w zasobniku będącym na wyposażeniu samolotu lub drona) większej ilości drobniejszej amunicji, która jest rozrzucana nad celem na zaprogramowanej wysokości i ma zdolność do rażenia większego wycinka terenu.

Miny przeciwpiechotne

Mina to każdy środek wybuchowy umieszczony pod powierzchnią lub na powierzchni ziemi (a także – na innych powierzchniach), który detonuje samodzielnie lub na zadany sygnał w sytuacji bliskości lub zetknięcia się z nim osoby czy pojazdu. Z wojskowego punktu widzenia wprowadza się różne kryteria podziału min.

Te podziały okazują się niezwykle istotne, gdyż wpływają na to, które normy MPH odnoszące się do konfliktów zbrojnych należy zastosować do danego rodzaju środka wybuchowego.

Jeden z nich dzieli miny na przeciwpiechotne (przeznaczone do rażenia siły żywej przeciwnika) oraz przeciwpancerne (służące do zwalczania pojazdów). Te pierwsze konstruuje się jako miny fugasowe, w których czynnikiem rażenia jest sama energia pochodząca z wybuchu, oraz jako miny odłamkowe, w których ta energia służy przede wszystkim do wyrzucenia metalowych elementów umieszczonych w takiej minie, zdolnych do rażenia przeciwnika, nawet na znaczne odległości.

W drugim podziale bierze się pod uwagę sposób stawiania miny. Pod tym względem wyróżnić można miny rozmieszczane ręcznie (stawiane przez saperów lub przez specjalistyczne maszyny, w tym – wykonujące tzw. minowanie narzutowe, przy czym miotanie min następuje na niewielką odległość) oraz miny stawiane zdalnie (za pomocą śmigłowców, samolotów, jak również artylerii lufowej i rakietowej).

Trzeci podział odnosi się do sposobu działania zapalnika i uwzględnia miny działające automatycznie, czyli z wykorzystaniem zapalników kontaktowych (naciskowych i naciągowych) albo niekontaktowych (magnetycznych i akustycznych, wykorzystywanych w minach przeciwpancernych), oraz wymagające aktywności człowieka, czyli są detonowane przewodowo lub radiowo.

2. Cyberatak na Estonię w 2007 roku

Na podstawie: J. Jalonen, *Dni, które wstrząsnęły Estonią*,
www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html

Wiosną 2007 roku po raz pierwszy w historii doszło do zmasowanego cyberataku przeciw suwerennemu państwu. Agresja, która miała wspomóc działania prowadzone przez Rosję w rzeczywistości realnej, zapoczątkowała nowy wyścig zbrojeń.

Gdy estoński rząd zaczynał przygotowania do przeniesienia tzw. Brązowego Żołnierza, czyli pomnika upamiętniającego sowieckich żołnierzy, poległych podczas „wyzwalania Tallinna z rąk nazistów" (jak twierdzi Kreml) albo – jak widzą to Estończycy – podczas ponownego podbijania ich kraju przez ZSRR, spodziewano się rytualnych protestów Moskwy. Nikt nie przypuszczał, nawet w najśmielszych wyobrażeniach, jaki charakter przybierze rosyjska reakcja.

Pierwsza cyberwojna w dziejach

Planom usunięcia pomnika z centrum Tallinna (na miejscowy cmentarz wojskowy) sprzeciwiali się też działacze mniejszości rosyjskiej w Estonii. Na początku ich protest miał jednak charakter pokojowy.

Dopiero gdy Rosja przedstawiła Estonii oficjalne ultimatum (że Brązowy Żołnierz ma zostać tam, gdzie stoi), sytuacja zamieniła się w międzynarodowy kryzys. Przez dwie noce, z 26 na 27 oraz z 27 na 28 kwietnia, estońską stolicą wstrząsały potężne zamieszki, prowokowane przez rosyjską młodzież. W tym czasie w Moskwie prokremlowska organizacja młodzieżowa zablokowała estońską ambasadę.

Podczas gdy na ulicach estońscy Rosjanie walczyli z policją, polem bitwy elektronicznej stał się estoński internet. Już 27 kwietnia o godzinie 22.30 serwis rządu zaczęły bombardować tzw. ataki *distributed denial of services* (DDoS). Dziś wiadomo, że te cyberataki, prowadzone przez wielu niezależnych hakerów, rozpoczęła rosyjska organizacja „Nasi", podporządkowana Kremlowi (ona sama utrzymuje, że jest niezależna od rosyjskiego rządu).

Od tamtego wieczora fala cyberataków na infrastrukturę informatyczną się nasilała: unieruchomiono strony internetowe parlamentu, ministerstw obrony i sprawiedliwości, partii politycznych, policji, a nawet szkół publicznych. Cyberataki osiągnęły apogeum 9 maja (rosyjski Dzień Zwycięstwa), gdy ich celem stał się też sektor prywatny. Sytuacja zaczęła przypominać powieść science fiction: dwa największe banki – Hansapank i SEB Ühispank – musiały zawiesić usługi online i wstrzymać transakcje zagraniczne. Zamarła też strona największego dziennika – „Postimees".

Wizja epoki kamiennej

Cyberwojna trwała trzy tygodnie. W tym czasie, po początkowym zaskoczeniu, szybko utworzona jednostka (Estonian Computer Emergency Response Team, CERT-EE), kierowana przez Hillara Aarelaida, miała ręce pełne roboty – musiała zorganizować obronę improwizowaną, ale – ostatecznie – efektywną. Aż do chwili, gdy 18 maja ataki nagle przerwano.

Ich cel został jednak osiągnięty: pokazano, jak bezbronne wobec cyberterroryzmu jest społeczeństwo małego kraju. Prezydent Toomas Hendrik Ilves powiedział potem: „W obecnych czasach nie potrzeba pocisków, żeby zniszczyć infrastrukturę. Można to zrobić online". Jeszcze bardziej ponuro zabrzmiał komentarz Gadiego Evrona, izraelskiego eksperta ds. bezpieczeństwa, w tym czasie przebywającego w Estonii: „Za pomocą cyberbomby Estonia została niemal zepchnięta do epoki kamiennej".

Dla zwykłego Estończyka cyberataki były raczej frustrujące niż niebezpieczne. Choć ich zakres spowodował też szkody finansowe (np. banków), to zastosowano w nich dość prymitywne metody, które nie wystarczyłyby do zniszczenia infrastruktury informatycznej estońskiego społeczeństwa. Pozostał jednak efekt psychologiczny: zawieszenie (nawet krótkotrwałe) usług bankowych wystarczyło, żeby zaniepokoić przeciętnego obywatela. Kiedy przestawały działać strony rządowe, informowanie obywateli o rozwoju sytuacji także stawało się trudniejsze, co mogło doprowadzić do wybuchu paniki – a na to prawdopodobnie liczyli napastnicy. Jednak większość Estończyków zachowała zimną krew – mimo cyberataków i zamieszania w rzeczywistości realnej.

Cyberatak odczuły dotkliwiej instytucje państwa. Estoński system obrony musiał na kilka dni zamknąć część połączeń zagranicznych. Oznaczało to izolację kraju od reszty świata. Swoiste cybernetyczne oblężenie uniemożliwiło też Estończykom podróżującym za granicę dostęp do ich kont bankowych. A zagraniczne biura podróży organizujące wycieczki do Estonii nagle odkryły, że ich system rezerwacji przestał funkcjonować.

Co mogłoby się stać…

Życie zwykłego obywatela zostało więc zakłócone jedynie nieznacznie. Jednak lęk przed tym, co mogłoby się stać, gdyby cyberataki były silniejsze i szerzej zakrojone, pozostał. Estonia jest wszakże krajem wysoce zinformatyzowanym, a banki, usługi, administracja i nawet system głosowania są ze sobą powiązane. Łatwo sobie wyobrazić, jakie skutki mógłby mieć skoncentrowany atak, wspierany przez pełne zasoby jakiegoś kraju.

Dlatego wydarzenia z wiosny 2007 roku estoński rząd potraktował poważnie. Podobnie zresztą postąpiło NATO, którego Estonia jest członkiem. Dyskutowano, czy artykuł piąty *Karty NATO* dotyczy także cyberwojny i cyberterroryzmu. A w 2008 r. właśnie Tallinn stał się siedzibą nowej NATO-wskiej instytucji: Cooperative Cyber Defence Centre

of Excellence, czyli ośrodka koordynującego obronę NATO-wskiej cyberprzestrzeni. Celem tego centrum nie jest tylko obrona – w przyszłości NATO ma być zdolne także do kontrataku.

Wydarzenia z wiosny 2007 roku i powołanie nowej instytucji zwróciły uwagę również Finlandii i Szwecji – krajów sąsiednich, ale nienależących do sojuszu. Ocena szwedzkiego centrum zarządzania kryzysowego nie napawa optymizmem: Szwecja nie tylko byłaby bezbronna wobec podobnego cyberataku, lecz także okazałaby się mniej zdolna niż Estonia do zorganizowania szybkiej obrony. Przeciwnie – Finlandia: to państwo ma powody do zadowolenia, gdyż fińskie systemy informatyczne są zdecentralizowane, co sprawia, że skoncentrowany atak stałby się trudniejszy do przeprowadzenia. Niemniej jesienią 2008 roku fiński rząd przeznaczył 197 mln euro na wzmocnienie bezpieczeństwa publicznego systemu informatycznego. A w rządowych raportach o zdolnościach obronnych kraju pojawił się nowy rozdział – dotyczący cyberwojny.

Nie udało się dowieść, że za cyberatakami na Estonię stał rosyjski rząd – jako np. ich zleceniodawca. Jednak faktem jest, że wydarzenia z wiosny 2007 roku rozpoczęły zupełnie nowy wyścig zbrojeń: odbywający się w cyberprzestrzeni. Bardziej niż tarcza antyrakietowa, to właśnie NATO-wskie centrum obrony cyberprzestrzeni w Estonii jest symbolem nowej i prawdziwie futurystycznej wizji tego, jak mogą wyglądać w przyszłości konflikty – także między państwami.

Na podstawie: *Kraj odporny na cyberataki. Jak Estonia poradziła sobie z rosyjskimi hakerami?*, ABB, 23 czerwca 2021, https://forsal.pl/lifestyle/technologie/artykuly/8194708,estonia-odporna-na-rosyjskie-cyberataki-doswiadczenia-kraju-krance-ue.html

Rozwój internetu i związana z tym cyfryzacja wielu kluczowych dziedzin światowej gospodarki wytworzyły nowe zjawisko, jakim stała się międzynarodowa cyberwojna. Nie są na nie odporne nawet takie potęgi jak Unia Europejska czy Stany Zjednoczone. Jest jednak jedno wyjątkowe państwo, które od ponad 20 lat prowadzi działania chroniące je przed cyberzagrożeniem ze strony Rosji. To Estonia.

Estonia to jeden z najbardziej cyfrowych krajów świata. Tam przez internet można załatwić w zasadzie każdą sprawę urzędową: od składania zeznań podatkowych, przez głosowanie, aż po rejestrację narodzin dziecka. Wysoki poziom bezpieczeństwa cybernetycznego oferowany przez systemy administracji rządowej regularnie plasuje Estonię na szczycie rankingów bezpieczeństwa. Zapewne jest to jeden z powodów stworzenia w stolicy centrum cyberobrony NATO. Cyberbezpieczeństwo stało się również jednym z priorytetów politycznych Tallinna podczas rotacyjnej prezydencji w Rady Bezpieczeństwa ONZ.

Estonia jest boleśnie świadoma cyberzagrożenia ze strony Rosji. Do zaostrzenia relacji i do największego cyberataku na pojedynczy kraj doszło w 2007 roku. Powodem eskalacji konfliktu były dyplomatyczne tarcia związane z decyzją o przeniesieniu pomnika wojennego z czasów sowieckich z centrum Tallina na cmentarz wojskowy. Estoński rząd nazwał ten incydent aktem cyberwojny, za który obwinił Rosję. Moskwa jednak zaprzeczyła jakiemukolwiek zaangażowaniu w atak hakerów. Podczas incydentu, trwającego 22 dni, nie wykradziono żadnych danych. Strony internetowe banków, mediów i niektórych służb rządowych były niedostępne. Sytuacja była na tyle poważana, że rząd w Tallinie zaczął traktować cyberzagrożenia w taki sam sposób, jak ataki fizyczne.

Od tego czasu kolejne rządy realizują szeroko zakrojoną krajową strategię cyberbezpieczeństwa. Tallinn wraz z prywatnymi firmami tworzy bezpieczne systemy teleinformatyczne. W Luksemburgu zbudowano „ambasadę danych" – specjalnie zabezpieczone centrum danych, w którym przechowuje się kopie zapasowe na wypadek cyberataku na obiekty na terytorium Estonii. Ten kraj stał się również jednym z pierwszych użytkowników technologii blockchain. Za pośrednictwem NATO i innych organizacji naciskał na większą globalną współpracę.

Najsłabsze ogniwo cybersystemu – człowiek

„Technologia daje nam wiele narzędzi do zabezpieczania systemu, ale ostatecznie poziom bezpieczeństwa zależy od użytkowników" – powiedział Sotiris Tzifas, ekspert ds. cyberbezpieczeństwa i dyrektor naczelny Trust-IT VIP Cyber Intelligence. Przeprowadzenie niektórych najbardziej szkodliwych cyberataków umożliwiali sami użytkownicy wewnętrzni, którzy klikali w łącza phishingowe, więc wcale nie potrzeba było wysoko wyspecjalizowanego hakera, korzystającego z najbardziej zaawansowanej technologii. Stzifas odniósł się również do cyberataku na rurociąg Colonial Pipeline. Ten atak zmusił amerykańską firmę do zamknięcia kluczowej instalacji na wschodnim wybrzeżu Stanów Zjednoczonych w kwietniu. „Atak zrobił dużo szumu i kosztował dużo pieniędzy, ale nie był bardzo skomplikowany, nie różnił się od innych ataków ransomware'owych" – uważa Tzifas.

Od lat estoński rząd inwestuje w programy edukacyjne i szkoleniowe. Zakres działań jest bardzo szeroki: od kampanii uświadamiających i warsztatów skierowanych do osób starszych po lekcje „kodowania" dla przedszkolaków.

Birgy Lorenz, ekspertka ds. cyberbezpieczeństwa z tallińskiej politechniki, jest inicjatorką wielu programów edukacyjnych w Estonii, których celem jest zapoznanie dzieci z najnowszymi technologiami, a także dostrzeżenie i wychowywanie przyszłych liderów technologii. Według Lorenz, małe dzieci chętnie uczą się o cyberbezpieczeństwie, jeśli zostaną zaangażowane w działania. „Tak naprawdę nie chcą słuchać, jak dorośli mówią im, co powinny robić, więc mówimy im, że potrzebujemy ich pomocy,

i prosimy, aby pomogły swoim rodzicom lub młodszej siostrze: przeprowadziły audyt wszystkich ich gadżetów i haseł, a potem pokazały domownikom, jak oni sami mogą to zrobić. Aby zdobyły pewne umiejętności i poczuły się odpowiedzialne za swoje cyberbezpieczeństwo" – powiedziała.

„Uczymy obrony, ale nie możesz nauczyć się obrony, jeśli nie wiesz, jak hakować" – uważa Lorenz. Zdobyciu wiedzy na ten temat służą temu specjalne obozy edukacyjne, na których nastolatki uczą się hakowania w bezpiecznym środowisku. Nikt jednak nie zachęca uczniów do łamania prawa czy do włamywania się na strony firm lub organów rządowych. Ale jeśli dojdzie do takiej sytuacji, to opiekunowie kontrolują sytuację i upewniają się, że młodzież zachowa się w sposób etyczny. Po czym informacja o wykryciu luki w zabezpieczeniu jest wysyłana do osób odpowiedzialnych za systemy.

Hakerzy na rządowej posadzie

W ciągu ostatnich kilku lat nastąpił duży wzrost liczby ataków sponsorowanych przez państwa. Rządy wykorzystywały działalność hakerów do wprowadzania chaosu w infrastrukturze strategicznej swoich przeciwników. W zeszłym roku USA i Wielka Brytania ostrzegły przed wzrostem wspieranych przez rządy cyberataków na organizacje zaangażowane w walkę z pandemią koronawirusa.

Jak najlepiej zabezpieczyć krytyczną infrastrukturę kraju przed cyberzagrożeniem? Trzeba zrozumieć motywacje potencjalnych napastników, uważa Tzifas. „Są hakerzy sponsorowani przez rząd, którzy atakują, potem są oszuści próbujący osiągnąć swoje ekonomiczne cele, a potem masz dzieciaki lub mało doświadczonych hakerów, którzy próbują sprawdzić, czy mogą coś zrobić" – dodał. Niektóre rządy i firmy zachęcają tę ostatnią grupę do podejmowania prób włamania do swoich systemów w nadziei, że młodzi hakerzy pomogą im odkryć słabe strony zabezpieczeń. Ci, którzy odniosą sukces, mogą liczyć na nagrody.

Porażka przekuta w sukces

Estonia zbudowała bezpieczne systemy informatyczne, wspierała współpracę międzynarodową, wydała dużo pieniędzy i przeznaczyła czasu na szkolenie swoich obywateli. Jednak w świecie, w którym hakerzy są niemal zawsze o krok przed rządami, ten kraj nieustannie próbuje znaleźć sposoby na ulepszenie swojego systemu.

„Estonia wprowadziła cyfryzację znacznie wcześniej niż inne kraje, koncentrowała się na takich rzeczach, jak kształcenie online i internetowe usługi rządowe, a także przyjęła bardziej proaktywne podejście do technologii" – powiedziała Esther Naylor, analityk ds. międzynarodowych badań bezpieczeństwa w Chatham House. „Uznano, że musi to być bezpieczny kraj, aby obywatele chcieli korzystać z systemów internetowych, a przedsiębiorstwa chciały prowadzić działalność gospodarczą w Estonii… i myślę, że właśnie dlatego podejście Estonii jest często przedstawiane jako modelowe" – dodała.

3. Cyberatak na Gruzję podczas wojny z Rosją w 2018 roku

Na podstawie: C. Sweeney, *Rosja i Gruzja prowadzą PR-ową bitwę o serca i umysły*, 10 sierpnia 2008 roku, Reuters, www.reuters.com/article/europeCrisis/idUSLA536003

Uzbrojone nie tylko w broń, lecz także w agencje *public relations*, Rosja i Gruzja toczą wojnę propagandową, aby kształtować opinię publiczną w kraju i za granicą za pomocą ciągłego strumienia spornych faktów na temat ich konfliktu.

Walki wybuchły, po tym jak Gruzja próbowała odzyskać kontrolę nad Osetią Południową, małą prorosyjską separatystyczną prowincją, w czwartek wieczorem. Rosja, przez swoją południową granicę, wysłała czołgi i oddziały do Gruzji, aby odepchnąć wojska Tbilisi.

Obie strony zatrudniają brukselskich specjalistów od *public relations*. Zorganizowali oni kilkanaście konferencji dla światowych mediów, podczas których wysocy rangą przedstawiciele rządu starali się jako pierwsi przedstawić swoją wersję wydarzeń.

Ponieważ Rosja chce przekonać świat o swojej roli jako uczciwego pośrednika, niechętnie interweniuje przeciwko wymykającemu się spod kontroli gruzińskiemu prezydentowi, którego siły przeprowadziły czystki etniczne wśród ludności osetyjskiej.

Gruzja z kolei przedstawia się jako dzielny mały kraj walczący z odradzającym się rosyjskim niedźwiedziem i cierpiący wskutek niesprawiedliwej kary nałożonej przez Kreml z powodu swoich dążeń do stania się zachodnią demokracją i sojusznikiem NATO. Mikheil Saakashvili, ówczesny gruziński prezydent, szybko starał się przekonać świat o swojej walce w telewizyjnych wywiadach udzielonych globalnym nadawcom, takim jak CNN i BBC. Mówił, że jego kraj jest „w stanie wojny" z Rosją, i apelował o pomoc Zachodu. Nie pomogło to jednak w wyjaśnieniu wielu spornych faktów. Każda ze stron oskarżyła drugą o spowodowanie poważnych strat wśród ludności cywilnej, a dane dotyczące ofiar śmiertelnych i rannych bardzo się różniły. Gruzja podała, że w ciągu czterech dni walk zestrzeliła dziesięć rosyjskich myśliwców, ale rosyjscy oficjele ocenili tę liczbę na dwa. Obie strony spierały się nawet o to, czy gruzińskie zawieszenie broni jest w toku. Gruzja twierdziła, że przekazała rosyjskiemu ambasadorowi podpisaną notę od Saakaszwilego, nakazującą gruzińskim żołnierzom przerwanie ognia o 5.00 rano (01.00 GMT). Agencja Interfax cytowała rosyjskie ministerstwo spraw zagranicznych, które wkrótce potem poinformowało, że otrzymało notę, ale walki nadal trwają.

Na rosyjskich kanałach telewizyjnych pojawiły się wielkie nagłówki głoszące „ludobójstwo" w Osetii Południowej, z pośpiesznie montowanymi obrazami płaczących kobiet, zbombardowanych budynków i przerażonych dzieci. Z kolei w Gruzji, w momencie wybuchu konfliktu, działał tylko jeden kanał telewizyjny, a wszystkie rosyjskie

strony internetowe z domeną .ru zostały na krótko zablokowane, choć były już dostępne w niedzielę wieczorem.

Chociaż stolica separatystów – Cchinwali – nie była centrum walk, miasto legło w gruzach, a niezależne relacje stały się niemożliwe, ponieważ dziennikarze, fotografowie i kamerzyści schronili się pod ziemią, aby uniknąć ostrzału. „Miasto zamienia się w ludzkie piekło, wielu ludzi wciąż uwięzionych pod gruzami" – głosił pasek rosyjskiej państwowej anglojęzycznej telewizji Russia Today, która stara się nadawać za granicą linię Kremla. Sporne okazały się dane dotyczące liczby ofiar śmiertelnych. Południowoosetyjscy urzędnicy twierdzą, że w pierwszej nocy ostrzału rakietowego zginęło co najmniej 1400 osób, ale nie są w stanie tego w pełni potwierdzić. Separatyści utrzymują również, że około 30 tysięcy uchodźców uciekło na północ, choć inne raporty mówią o zaledwie ułamku tej liczby przybyłych do Osetii Północnej.

Świadom znaczenia Gruzji jako energetycznego korytarza tranzytowego prowadzącego z regionu kaspijskiego, bogatego w ropę naftową, na zachód, gruziński minister oskarżył Moskwę o próbę zbombardowania kluczowego ropociągu biegnącego przez jej terytorium. Rosja zaprzeczyła, że zaatakowała jakikolwiek cel niewojskowy, a niezależni eksperci zwrócili uwagę, że rurociąg i tak był już nieczynny z powodu eksplozji, która miała miejsce we wschodniej Turcji kilka dni wcześniej i poważnie go uszkodziła.

Gdy konflikt rozszerzył się na drugi gruziński region separatystyczny – Abchazję, Gruzja oskarżyła Rosję o to, że stoi ona za operacją wojskową prowadzoną przez separatystów i mającą na celu odzyskanie części terytorium od Gruzji, natomiast Moskwa zaprzeczyła jakiemukolwiek zaangażowaniu.

Nawet na morzu mgła wojny opadła w niedzielę. Kakha Lomaia, sekretarz Rady Bezpieczeństwa Gruzji, powiedział, że port Poti nad Morzem Czarnym, zbombardowany przez rosyjskie samoloty we wczesnych godzinach sobotnich, jest obecnie blokowany przez rosyjską marynarkę wojenną. Generał pułkownik Anatolij Nogowicyn, przedstawiciel rosyjskiego dowództwa, odrzucił to twierdzenie. Podkreślił, że przechwytywane są tylko transporty broni, choć Gruzja twierdziła, że zablokowano pszenicę i paliwo, a nie – broń.

Na podstawie: D. Hollis, *Studium przypadku cyberwojny: Gruzja 2008*, Small Wars Journal, 2011, https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Wojnę rosyjsko-gruzińską uznaje się za mającą znaczenie historyczne i precedensową z kilku powodów.

Wydaje się, że był to pierwszy w historii przypadek skoordynowanego ataku w domenie cyberprzestrzeni i zsynchronizowanego z głównymi działaniami bojowymi

w domenach tradycyjnych. Trzy tygodnie przed rozpoczęciem konfliktu zbrojnego między Gruzją a Rosją napastnicy internetowi zaczęli atakować strony internetowe Gruzji. Od tego czasu badacze starają się ustalić, kto kierował tymi atakami w sieci – wojskowi wojownicy elektroniczni, patriotyczni hakerzy, cyberprzestępcy, ale nie znajdują niczego konkretnego. Niemniej Rosja przeprowadziła inwazję na Gruzję na czterech frontach. Trzy z nich były konwencjonalne – na ziemi, w powietrzu i na morzu. Czwarty okazał nowy – ataki w cyberprzestrzeni. Jest po prostu niewiarygodne, że równoległe ataki lądowe i w cyberprzestrzeni były zbiegiem okoliczności – niezależnie od oficjalnych zaprzeczeń Moskwy.

(Rzekomy) rosyjski atak na gruzińskie sieci wojskowe i rządowe był bardzo udany. Wygląda na to, że 54 strony internetowe w Gruzji związane z komunikacją, finansami i rządem zostały zaatakowane przez nieuczciwe elementy w Rosji. Zatem gdy czołgi i wojska przekraczały granicę, a bombowce odbywały krótkie loty, gruzińscy obywatele nie mogli uzyskać dostępu do portali internetowych w celu uzyskania informacji i instrukcji. Władze gruzińskie odkryły, że ich dostęp do internetu i sieci komunikacyjne są wyjątkowo podatne na (rzekomą) ingerencję Rosji.

Był jeszcze jeden historycznie wyjątkowy i krytyczny aspekt tych walk – pojawienie się zsynchronizowanych działań w domenie cyberprzestrzeni jako wskaźnika wywiadowczego dla operacji wojskowych na poziomie strategicznym, operacyjnym i taktycznym. W przeciwieństwie do (rzekomego) rosyjskiego cyberataku na Estonię w 2007 roku, (rzekomemu) rosyjskiemu cyberatakowi na Gruzję towarzyszyła fizyczna walka między rosyjskimi a gruzińskimi siłami zbrojnymi. (Domniemane) rosyjskie operacje ataku sieciowego w wirtualnej cyberprzestrzeni miały miejsce przed działaniami wojennymi, a następnie stały się odzwierciedleniem (najwyraźniej zsynchronizowanych) rosyjskich operacji bojowych w domenie działań wojennych na lądzie.

Ten cyberatak obejmował różne rozproszone ataki typu DDoS, mające na celu uniemożliwienie lub zakłócenie łączności, jak również działania w zakresie eksfiltracji informacji, prowadzone w celu gromadzenia wojskowych i politycznych danych wywiadowczych pobranych z gruzińskich sieci. Ponadto należy w ten zakres włączyć niszczenie gruzińskich stron internetowych dla celów rosyjskiej propagandy. Jednym z pierwszych zaatakowanych elementów stało się popularne forum gruzińskich hakerów – próba zlikwidowania ich aktywności przez bojówki hakerów wspierane przez Rosję miała uprzedzić lub złagodzić kontratak (lub odwet) ze strony gruzińskich hakerów. I rzeczywiście – choć ta informacja nie przebiła się do opinii publicznej, to faktem jest, że progruzińscy hakerzy przeprowadzili ograniczone, ale udane kontrataki sieciowe przeciwko rosyjskim celom.

Na poziomie strategicznym (rzekome) rosyjskie ataki rozpoznawcze i sondujące w cyberprzestrzeni zaczęły się na wiele tygodni przed faktycznym rozpoczęciem wirtualnej i fizycznej walki. Na rosyjskich stronach internetowych, czatach i forach również z kilkutygodniowym wyprzedzeniem omawiano nadchodzące ataki. Zresztą rozpoczęły się one na kilka tygodni przed faktyczną „interwencją", kiedy to w lipcu stronę internetową prezydenta Gruzji zaatakowali rosyjscy hakerzy metodą DDoS, po czym w rosyjskiej sieci rozpoczęły się aktywne dyskusje na temat tego, czy ataki DDoS i niszczenie stron internetowych powinny faktycznie mieć miejsce – a takie komentarze nieuchronnie stałyby się poręcznym narzędziem do wykorzystania przeciwko Rosji przez zachodnich lub prozachodnich dziennikarzy. Wygląda na to, że (rzekomi) rosyjscy napastnicy przeprowadzili próbę generalną swojego zsynchronizowanego cyberataku na początku lipca 2008 roku.

Warto też odnotować, że na tygodnie przed tym, jak bomby zaczęły spadać na Gruzję, badacz bezpieczeństwa mieszkający na przedmieściach Massachusetts obserwował atak na ten kraj w cyberprzestrzeni. Jose Nazario z Arbor Networks w Lexington zauważył strumień danych skierowany na gruzińskie strony rządowe, zawierający wiadomość: „win+love+in+Rusia". Inni eksperci internetowi w Stanach Zjednoczonych stwierdzili, że ataki na gruzińską infrastrukturę internetową rozpoczęły się już 20 lipca, od skoordynowanej zapory milionów żądań – znanej jako rozproszona odmowa usługi (DDoS) – która przeciążyła i skutecznie wyłączyła gruzińskie serwery. Jak się okazuje, lipcowy atak mógł być próbą generalną cyberwojny po rozpoczęciu ostrzału między Gruzją a Rosją. Według ekspertów z dziedziny techniki internetowej, był to pierwszy znany przypadek cyberataku, który zbiegł się w czasie z wojną kinetyczną.

4. Stuxnet i cyberwojna między USA a Iranem

Na podstawie: Bartosz Józefiak, *Stuxnet nie zniknął. Infrastruktura krytyczna nadal narażona na cyberatak*, 15 czerwca 2016,
https://cyberdefence24.pl/stuxnet-nie-zniknal-infrastruktura-krytyczna-nadal-narazona-na-cyberatak

Zarządcy infrastruktury krytycznej często żyją w przekonaniu, że ich systemy są wolne od zagrożenia cyberatakami, bo nie są podłączone do sieci. Jednak w 95% przypadków są w błędzie – przekonują eksperci. Zagrożenia takie jak wirus Stuxnet czy wirusy ransomware mogą wyrządzić ogromne szkody, ponieważ nawet chwilowe wyłączenie procesów przemysłowych będzie oznaczało ogromne straty dla przedsiębiorstwa.

– Cyberzagrożenia to już nie jest tylko zadanie działów IT. Niemal każda część firmy powinna być zaangażowana w cybersecurity. Eksperci od zarządzania ryzykiem, prawnicy, specjaliści od ubezpieczeń, kadra zarządzająca, finanse… Jest wiele aspektów, które trzeba rozważyć – mówił podczas wczorajszej konferencji

„Cyberbezpieczeństwo przemysłu i infrastruktury krytycznej" Andriej Suworow, zajmujący się ochroną infrastruktury krytycznej w Kaspersky Lab.

Suworow tłumaczył, że dzisiaj przeciwnikiem nie jest zespół hakerów, który zajmuje się po prostu pisaniem kodu. To dobrze zorganizowane grupy, które prowadzą wnikliwe śledztwa dotyczące systemów atakowanej firmy, luk w zabezpieczeniach, zachowań pracowników. Dlatego obecnie działania powinny być nakierowane na detekcję wszelkich anomalii i dziwnych zachowań w systemie, a nie – tylko na zwykłe odpieranie potencjalnych ataków.

Jaka różnica zachodzi między ochroną sieci przemysłowej a ochroną sieci innych firm? W typowej sytuacji priorytetem jest zachowanie poufności danych. Chodzi o to, żeby wiadomości z firmy nie wychodziły na zewnątrz. Dla infrastruktury krytycznej i przemysłowej najważniejsze okazuje się zachowanie ciągłości procesów. – Mamy klientów, których nawet jedna sekunda przerwy w dostawie energii może kosztować mnóstwo pieniędzy – tłumaczy Suworow.

Klasycznym przykładem zagrożenia dla infrastruktury krytycznej jest wirus Stuxnet, którego koalicja USA i Izraela użyła do ataku na instalacje wzbogacania uranu Islamskiej Republiki Iranu. Wykorzystano wtedy zarażony pendrive, wniesiony do instalacji przez nieświadomego pracownika. Stuxnet otworzył agresorom dostęp do technologii procesów, którą mogli zmienić, aby użyć jej do własnych celów. Kto uważa, że było to jednorazowe zagrożenie, ten jest w błędzie. Poza Iranem ten wirus wykryto w 15 krajach. Jest on wciąż powielany i wykorzystywany do kolejnych ataków. – Dwa miesiące temu znaleźliśmy jego ślady w rosyjskiej firmie przemysłowej – opowiada Suworow.

Do tego dochodzi także zagrożenie wirusami typu ransomware. Przestępcy nie mają żadnych skrupułów i zdarzały się już ataki zatrzymujące zakłady przemysłowe. Ich ponowne uruchomienie jest uzależnione od okupu wpłaconego na konta przestępców.

Większość systemów infrastruktury krytycznej projektowano bez znajomości cyberzagrożeń. Hakerom coraz częściej udaje się przejąć kontrolę nad linią technologiczną. Od spenetrowania systemu do wywołania incydentu mija około 14 godzin. Dobra wiadomość jest taka, że każda operacja hakerów jest podzielona na kilka stopni. Jeżeli wykryje się ją w odpowiednim momencie, uda się przeszkodzić rozwojowi zagrożenia.

Zarządcy infrastruktury krytycznej często żyją w przekonaniu, że ich systemy są bezpieczne, skoro nie są podłączone do sieci. – W 95% przypadków jesteśmy w stanie udowodnić naszym klientom, że jednak są podłączeni, a tym samym stają się zagrożeni – tłumaczy Suworow.

Na podstawie: Warsaw Institute, *Witajcie w cyberwojnie. USA vs. Iran. Raport specjalny*, 2020, https://warsawinstitute.org/wp-content/uploads/2020/12/Witajcie-w-cyberwojnie-Wiktor-Sedkowski-Raport-Specjalny-Warsaw-Institute-17.12.2020.pdf

Cyberwojnę między USA a Iranem uważa się za pierwszy konflikt cybernetyczny. Rozpoczęła się ona od ataku wirusa Stuxnet na infrastrukturę irańskiego programu nuklearnego. Iran odpowiedział atakiem na sektor prywatny w USA oraz w krajach będących sojusznikami Ameryki. Przykładowo: 15 sierpnia 2012 roku, pod nieobecność załogi Saudi Aramco, wirus Shamoon przystąpił do operacji kasowania danych z dysków twardych.

Cyberoperacje wywiadowcze stanowią tylko jeden z rodzajów aktywności w cybernetycznym arsenale. Obie strony konfliktu między USA a Iranem korzystały z różnych środków. Najbardziej znanym był wspomniany wcześniej Stuxnet – jego zadaniem było uniemożliwienie Iranowi rozwoju programu nuklearnego. Stuxnet wykorzystywał nie tylko nieznane szerzej podatności systemu operacyjnego, lecz także luki w bezpieczeństwie niektórych sterowników, stanowiących integralną część systemów w irańskim ośrodku nuklearnym Natanz.

W wyniku użycia tego wirusa udało się zniszczyć niespełna tysiąc wirówek w zakładzie wzbogacania uranu, co opóźniło program nuklearny Iranu o ponad 5 lat. Twórcy Stuxnetu nie osiągnęli swojego celu niskim kosztem: rozwój tak skomplikowanego rozwiązania pochłonął środki przekraczające co najmniej kilkadziesiąt milionów dolarów. Precyzyjne uderzenie wymagało pracy nie tylko programistów, lecz także ekspertów dysponujących wiedzą na temat specjalistycznych systemów i samych sterowników.

Z całą pewnością wirus został dokładnie przetestowany, zanim uderzył, tak więc zakup samych wirówek P1 używanych w Natanz należało sfinansować z budżetu przeznaczonego na rozwój cyberbroni. Iran odpowiedział atakiem na sektor prywatny w USA. W 2012 roku zaatakowane zostały amerykańskie banki. Atak DDoS, niezbyt skomplikowany z technicznego punktu widzenia, uniemożliwił klientom amerykańskich instytucji finansowych m.in. korzystanie z systemów bankowości elektronicznej. Trwał przez niemal pół roku i w tym czasie dotknął 46 instytucji finansowych (m.in. Bank of America, JPMorgan czy NASDAQ). Pomimo swojej prostoty wyrządził szkody wyceniane na dziesiątki milionów dolarów. Odpowiedzialna za atak grupa Izz ad-Din al-Qassam Cyber Fighters utrzymywała, że powodem był antymuzułmański film zamieszczony w serwisie YouTube. Eksperci w dziedzinie cyberbezpieczeństwa oraz agenci służb wywiadowczych są jednak zgodni, że był to odwet za Stuxnet, zresztą całkiem udany, jeśliby uwzględnić stosunek kosztów do wyrządzonych zniszczeń.

Iran otrzymał kolejny cios w 2012 roku. Złośliwe oprogramowanie Wiper uderzyło głównie w sektor produkcji ropy w Iranie: nieodwracalnie skasowało dane z tysięcy

maszyn, co przyczyniło się do podjęcia decyzji o odłączeniu wielu systemów od sieci internetowej. Dane usunięte przez malware przepadły na zawsze, tak samo jak informacja o jego autorach. Firma Kaspersky próbowała powiązać kod Wipera ze Stuxnetem, jednak oficjalnie nikt nie przyznał się do finansowania tej operacji.

Podobnie nieznani są autorzy wirusa Shamoon, który kilka miesięcy po ataku Wipera sparaliżował działalność globalnego lidera w produkcji ropy – Saudi Aramco. Ślady wskazują na Iran, który miał oczywisty powód do zaatakowania sojusznika Stanów Zjednoczonych. Saudi Aramco straciło ponad 30 tysięcy komputerów, wszystkie kluczowe systemy i dane. Sytuacja była na tyle poważna, że aby zapewnić ciągłość dostaw, zdecydowano się na wysyłanie ropy bez procesowania dokumentów finansowych (liczono przy tym na uczciwość kontrahentów).

Polityczny powód ataku było dosłownie widać gołym okiem. Oto 15 sierpnia 2012 roku 50 tysięcy pracowników firmy świętowało jedno z najważniejszych wydarzeń w kulturze muzułmańskiej – Noc Przeznaczenia. Pod nieobecność załogi Shamoon przystąpił do operacji kasowania danych z dysków twardych, na każdym z nich pierwsze 1024 bajty zostały nadpisane plikiem graficznym przedstawiającym płonącą amerykańską flagę. Oprócz Saudi Aramco, w ataku ucierpiały także systemy katarskiego RasGas, producenta i eksportera ciekłego gazu ziemnego. Efekt ataku był odczuwalny na zupełnie innym rynku. Saudi Aramco, aby przywrócić operacyjność systemów, natychmiastowo zamówiło u producentów sprzętu komputerowego dziesiątki tysięcy dysków twardych, co – również w konsekwencji ówczesnych powodzi w Azji – odbiło się na globalnej dostępności tych podzespołów i na ich cenach.

W 2017 roku pojawiła się nowa wersja wirusa Shamoon i tym razem niemal doprowadziło to do eksplozji w saudyjskiej rafinerii. Wzmożona aktywność Iranu w cyberprzestrzeni obrała za cel nie tylko sojuszników Zachodu, lecz także bezpośrednio Stany Zjednoczone. Dzień po tym jak prezydent Donald Trump podjął decyzję o wycofaniu się z porozumienia nuklearnego z Iranem (JCPOA), sieć wypełniła się od phishingowych maili, którymi irańscy hakerzy próbowali zwabić ofiary powiązane z administracją rządową i z innymi amerykańskim instytucjami. Amerykanom udało się obronić przed zdecydowaną większością ataków – jednak nie przed wszystkimi. Urzędy w Atlancie zainfekowane przez ransomware irańskiego pochodzenia nie mogły przez wiele dni świadczyć usług. Dwóch irańskich hakerów oskarżono o atak, a jego skutki wyceniono na 17 milionów dolarów. Podobna historia miała miejsce w Baltimore w maju 2019, wtedy koszt wyniósł 6 milionów dolarów. Według Microsoftu, w latach 2017–2019 irańskie cyberoperacje obrały za cel ponad 200 firm i instytucji w Stanach Zjednoczonych.

Siły amerykańskie nie pozostawały dłużne i realizowały własne cyberoperacje w Iranie. O większości z nich zapewne jeszcze przez dłuższy czas opinia publiczna się nie

dowie, jednak wielokrotnie pojawiały się informacje na temat zakłóceń pracy systemów infrastruktury krytycznej w Iranie, jak chociażby wspomniany wypadek w Natanz z lipca 2020 roku. Warto wspomnieć, że do walki po stronie USA włączyli się też cywilni aktywiści.

W 2018 roku kilka tysięcy urządzeń w Iranie wyświetliło flagę Stanów Zjednoczonych z napisem „Nie mieszajcie się w nasze wybory!". Było to działanie nieznanej grupy, która wykorzystała luki w oprogramowaniu routerów i zostawiła tę informację nie tylko w Iranie, lecz także m.in. na tysiącach maszyn w Chinach.

5. Przykłady badań i eksperymentów ukierunkowanych na doskonalenie żołnierzy

- **Środki stymulujące**: kiedyś amfetamina, dzisiaj modafinil – wzmacniają uważność, ogólną kognitywną i fizyczną wydajność, nawet w razie niedoboru snu
- **Wzmocnienie neuronalne**: podczaszkowy czip (zdalnie sterowany, umożliwiający przesyłanie sygnałów bezpośrednio z mózgu, interfejs człowiek – maszyna), nieinwazyjna stymulacja mózgu (porażenie prądem elektrycznym powodujące pobudzenie do 30h), przezczaszkowa stymulacja magnetyczna (wzmocnienie pamięci i uważności np. wśród operatorów dronów).
- **Wzmocnienie fizyczne**: wzmocnienie kręgosłupa (możliwość udźwignięcia większych ciężarów), egzoprotezy i endoprotezy bioniczne (wsparcia inwalidów).
- **Inne badania**: przemiana celulozy krystalicznej w glukozę (umożliwia jedzenie trawy i innych niestrawnych roślin), rozpoznawanie optyczne wspomagane przez człowieka (neurooptyczne okulary), tzw. prawdziwy nos (nos jak u psa, umożliwia rozpoznanie większej gamy zapachów), Z-Man (chodzenie po ścianach jak jaszczurka).

Materiały dla nauczycieli

1. Klasyczne środki walki

Umowy międzynarodowe wprowadzające zakazy i ograniczenia w zakresie używania niektórych środków walki:

- Deklaracja w sprawie pocisków wybuchających małego kalibru, tzw. deklaracja petersburska z 29 listopada (11 grudnia) 1868 r., zabraniająca używania pocisków wagi mniejszej niż 400 g.
- Deklaracja petersburska z 1899 r. o zakazie zrzucania z balonów pocisków i materiałów wybuchowych.
- Konwencja dotycząca praw i zwyczajów wojny lądowej podpisana wraz z odnośnym regulaminem w Hadze dnia 18 października 1907 r., Dz.U. Nr 21 z 1927 r., poz. 161.
- Protokół dotyczący zakazu używania na wojnie gazów duszących, trujących lub podobnych oraz środków bakteriologicznych, przyjęty w Genewie dnia 17 czerwca 1925 r., Dz.U. Nr 28 z 1929 r., poz. 278.
- Konwencja o zakazie prowadzenia badań, produkcji i gromadzenia zapasów broni bakteriologicznej (biologicznej) i toksycznej oraz o ich zniszczeniu, sporządzona w Moskwie, Londynie i Waszyngtonie 10 kwietnia 1972 r., Dz.U. Nr 1 z 1976 r., poz. 1.
- Konwencja o zakazie używania technicznych środków oddziaływania na środowisko w celach militarnych lub jakichkolwiek innych celach wrogich, sporządzona w Genewie dnia 18 maja 1977 r., Dz.U. Nr 31 z 1978 r., poz. 132.
- Protokół dodatkowy do konwencji genewskich z 12 sierpnia 1949 roku, dotyczący ofiar międzynarodowych konfliktów zbrojnych, sporządzony w Genewie dnia 8 czerwca 1977 r., Dz.U. Nr 41 z 1992 r., poz. 175.
- Konwencja o zakazie lub ograniczeniu użycia pewnych broni konwencjonalnych, które mogą być uważane za powodujące nadmierne cierpienia lub mające niekontrolowane skutki, zawarta w Genewie dnia 10 października 1980 r., 1342 UNTC 137.
  - Protokół I w sprawie niewykrywalnych odłamków
  - Protokół II z 10 października 1980 r. i poprawiony protokół II z 3 maja 1996 r. w sprawie zakazów lub ograniczeń użycia min, min pułapek i innych urządzeń
  - Protokół III w sprawie zakazów lub ograniczeń użycia broni zapalających
  - Protokół IV z 13 października 1995 r. w sprawie laserowych broni oślepiających

  - Protokół V z 28 listopada 2003 r. w sprawie wybuchowych pozostałości wojennych.
- Konwencja o zakazie broni chemicznej, podpisana w Paryżu dnia 13 stycznia 1993 r., Dz.U. Nr 63 z 1999 r., poz. 703.
- Konwencja o zakazie użycia, składowania, produkcji i transferu min przeciwpiechotnych oraz o ich zniszczeniu, przyjęta w Oslo dnia 18 września 1997 r., 2056 UNTC 211.
- Konwencja o zakazie produkcji, składowania i używania bomb i pocisków kasetowych, podpisana w Oslo dnia 23 grudnia 2008 r., 2688 UNTC 39.
- Traktat zakazujący broni jądrowej, sporządzony w Nowym Jorku dnia 7 lipca 2017 r.
- Układ o nierozprzestrzenianiu broni jądrowej, sporządzony w Moskwie, Waszyngtonie i Londynie dnia 1 lipca 1968 r., Dz.U. Nr 8 z 1970 r., poz. 60.
- Traktat o całkowitym zakazie prób z bronią jądrową, sporządzony w Nowym Jorku dnia 24 września 1996 r.
- Konwencja w sprawie zakazu stosowania tortur oraz innego okrutnego, nieludzkiego lub poniżającego traktowania albo karania, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 10 grudnia 1984 r., 1465 UNTC 85.

2. Nowe środki walki

Nowymi środkami walki nazywa się zbiorczo takie typy broni, które dotychczas nie zostały uregulowane w umowach międzynarodowych, a do których stosuje się podstawowe zasady MPH (zasada rozróżnienia, środki ostrożności, zakaz powodowania zbędnego cierpienia i nadmiernego okrucieństwa). Możliwości, które oferuje współcześnie rozwijana technologia, w znacznym stopniu wpływają na to, jak postrzegamy powyższe zasady i w jaki sposób są toczone współczesne konflikty zbrojne.

- **Cyberbroń**
  Walka cybernetyczna, odbywająca się przy użyciu sieci komputerowej i różnych szkodliwych programów, może doprowadzić do poważnego zagrożenia dla bezpieczeństwa państwa bez uciekania się do siły zbrojnej.

  Wymownymi przykładami były paraliż platform państwowych w wyniku ataku na Estonię w 2007 roku, dezinformacja (połączona z działaniami zbrojnymi) w wyniku ataków na strony rządowe podczas wojny między Gruzją a Rosją w 2008 roku czy zmiana sposobu funkcjonowania kluczowych elementów elektrowni jądrowej w Iranie w wyniku zainstalowania robaka komputerowego, którego działanie wykryto w 2010 roku.

Ataki na infrastrukturę krytyczną (np. sieci zasilające, główne węzły komunikacyjne, systemy informatyczne) wydają się w tym zakresie szczególnie niebezpieczne, gdyż mogą doprowadzić do destabilizacji w kraju na masową skalę, czemu towarzyszyłby efekt zaskoczenia – co w rezultacie może się okazać bardzo skuteczną taktyką, zwłaszcza w państwach o niskiej kulturze bezpieczeństwa cybernetycznego.

Centrum obrony cybernetycznej NATO z siedzibą w Tallinnie zleciło ekspertom z zakresu międzynarodowego prawa humanitarnego przygotowanie analizy objaśniającej zastosowanie obowiązującego prawa międzynarodowego w kontekście ataków w cyberprzestrzeni. W ten sposób powstały *Podręczniki tallińskie* (pierwszy z 2013 roku na temat kontekstu konfliktów zbrojnych oraz drugi z 2017 roku na temat ataków poniżej progu wojny). Do dzisiaj nie zawarto żadnej umowy międzynarodowej z zakresu międzynarodowego prawa humanitarnego, która byłaby poświęcona cyberwojnie.

- **Bronie autonomiczne**
  Używanie sztucznej inteligencji do działań bojowych stało się jednym z zagadnień, które doczekały się najszerzej zakrojonej dyskusji międzynarodowej na temat możliwości regulacji tych środków walki w traktacie. Stało się tak dzięki działaniom Kampanii przeciwko Robotom Zabójcom – międzynarodowej koalicji organizacji pozarządowych, działającej od 2013 roku i podkreślającej ryzyko wynikające z oddania decyzyjności maszynom.

  Do dzisiaj nie przyjęto w tej kwestii żadnego wiążącego instrumentu prawa międzynarodowego, jednak podkreśla się, że w sytuacjach wymagających używania sztucznej inteligencji, która nie dorównuje ludziom i ich zdolnościom, to człowiek powinien zawsze sprawować znaczącą kontrolę nad systemami uzbrojenia wyposażonymi w sztuczną inteligencję. Taka idea ma na celu umożliwienie przypisania odpowiedzialności w razie naruszeń MPH, które miałyby miejsce w wyniku działania takich systemów. Jak do tej pory nie rozstrzygnięto, czy zastosowanie sztucznej inteligencji byłoby korzystniejsze z myślą o ograniczeniu cierpienia i strat wojennych, gdyby osiągnęła ona wystarczający poziom skuteczności (np. gdyby popełniała ona mniej błędów podczas walki niż żołnierze).

- **Doskonalenie żołnierzy**
  Wzmacnianie zdolności i umiejętności żołnierzy stało się nieodłącznym elementem szkolenia. O ile w przeszłości o przewadze wojskowej decydowała liczebność armii, o tyle wraz z rewolucją przemysłową, która zmieniła charakter konfliktów zbrojnych, to śmiercionośna technologia przesądzała o wyniku działań

wojennych. Nowe zjawiska związane z obronnością, takie jak profesjonalizacja armii, wyścig zbrojeń, rosnące znaczenie jednostek specjalnych (ale także – prywatnych spółek wojskowych), przyczyniły się do powstania kolejnego trendu, jakim jest technologiczne doskonalenie żołnierza (ang. *human enhancement*). W tym wypadku człowiek ma zostać pozbawiony przymiotu miana najsłabszego ogniwa w armii.

Doskonalenie żołnierzy może mieć różną formę (podstawową jest trening), przy czym obecnie mówi się o coraz bardziej zaawansowanym połączeniu człowieka z technologiami, które może doprowadzić do traktowania ludzi jako elementu wyposażenia armii (ekwipunku).

Technologie doskonalenia żołnierzy (HET, ang. *human enhancement technologies*) przekraczają granice biotechnologii i wpływają na naturę konfliktów zbrojnych, stosunków międzynarodowych i geopolityki. W przeciwieństwie do terapii ukierunkowanych na naprawę lub wyleczenie uszkodzonego ciała lub psychiki, HET stymulują i doskonalą ludzkie ciało ponad naturalne zdolności (w sposób odwracalny lub nieodwracalny). Mają przy tym różnorakie działanie, m.in. wzmacniają siłę mięśni, zarządzają bólem, nadzwyczajną czujnością, pamięcią. Ich wspólnym celem jest wypracowanie szybszego, lepszego i tańszego sposobu na osiągnięcie sukcesu w konflikcie zbrojnym.

Zasoby internetowe

Międzynarodowe prawo humanitarne konfliktów zbrojnych, red. Z. Falkowski, M. Marcinko, Warszawa 2014, https://wceo.wp.mil.pl/y/pliki/rozne/2019/07/MPHKZ.pdf

Systemy dronów bojowych. Analiza problemów i odpowiedź społeczeństwa obywatelskiego, red. K. Kowalczewska, J. Kowalewski, Warszawa 2015, www.academia.edu/41420561/Systemy_Dron%C3%B3w_Bojowych._Analiza_problem%C3%B3w_i_odpowied%C5%BA_spo%C5%82ecze%C5%84stwa_obywatelskiego_red._K._Kowalczewska_J._Kowalewski

Vademecum bezpieczeństwa, red. O. Wasiuta, R. Klepka, R. Kopeć, Kraków 2018, https://depot.ceon.pl/handle/123456789/16331

Łukasz Kamieński, *Nowy wspaniały żołnierz*, Kraków 2014, https://wuj.pl/ksiazka/nowy-wspanialy-zolnierz

Kaja Kowalczewska, *Sztuczna inteligencja na wojnie*, Warszawa 2021, https://scholar.com.pl/pl/ksiazki/4185-sztuczna-inteligencja-na-wojnie.html

Janusz Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" vol. 5(9), 2013, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-fad9287e-d6f2-4713-ad9e-472717378ab4

Przemysław Roguski, *Russian Cyber Attacks against Georgia, Public Attributions and Sovereignty in Cyberspace*, "Just Security" 2020, www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace

Tomasz Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego", vol. 8(15), 2016, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-c40b3292-a776-4b3a-97b3-978008a6860b

Bronie, Międzynarodowy Komitet Czerwonego Krzyża www.icrc.org/en/war-and-law/weapons

Cyberoperacje podczas konfliktów zbrojnych, Międzynarodowy Komitet Czerwonego Krzyża, www.icrc.org/en/war-and-law/conduct-hostilities/cyber-warfare

Nowe technologie i MPH, Międzynarodowy Komitet Czerwonego Krzyża www.icrc.org/en/war-and-law/weapons/ihl-and-new-technologies

O autorce

Kaja Kowalczewska – doktor nauk prawnych, wykładowca akademicki, radca prawny. Autorka scenariuszy zajęć, warsztatów i kursów z zakresu międzynarodowego prawa humanitarnego przeznaczonych dla nauczycieli, studentów oraz młodzieży szkolnej, i prowadząca te zajęcia. Członkini Komisji ds. Upowszechniania Międzynarodowego Prawa Humanitarnego przy Zarządzie Głównym Polskiego Czerwonego Krzyża.

Ośrodek Rozwoju Edukacji
Aleje Ujazdowskie 28
00-478 Warszawa
tel. 22 345 37 00; fax 22 345 37 70

www.ore.edu.pl