TRANSKRYPCJA – Odcinek XI

Wojna obrony cyberprzestrzeni

[00:00:06]

Prowadzący: Cześć. Witam wszystkich słuchaczy w kolejnym odcinku naszego podcastu. I dzisiaj kolejny raz poruszymy kwestię obrony przed cyberprzestępcami. Tym razem nie tyle skierowaną do pojedynczej organizacji, co uderzającą wprost w obronność kraju. Jak wygląda szkolnictwo w tym zakresie, jak państwo przygotowuje do służby ojczyźnie nie tylko zwykle w stanie konwencjonalnej broni? Czy może nam grozić globalny cyberkonflikt? O tym już za chwilę. Cyberbezpieczeństwo kraju, rozszerzenie możliwości militarnych. Zaczynamy. Moim dzisiejszym gościem jest płk dr inż. Rafał Kasprzyk. Absolwent Wydziału Cybernetyki Wojskowej Akademii Technicznej, obecny zastępca dziekana Wydziału Cybernetyki. Panie Rafale, jest mi naprawdę niezmiernie miło móc Pana dzisiaj gościć z nami.

Płk dr inż. Rafał Kasprzyk: Witam Pana bardzo serdecznie. Witam Państwa.

Prowadzący: Panie Rafale, zanim przejdziemy do głównego tematu naszego dzisiejszego odcinka, chciałbym zapytać Pana, jako absolwenta WAT na Wydziale Cybernetyki, skąd właśnie ta ścieżka? Jak to się u Pana narodziło? Skąd właśnie cybernetyka i wojskowa uczelnia?

Płk dr inż. Rafał Kasprzyk: Tak, tutaj właściwie dwie perspektywy. Pierwsza perspektywa daleka od tego odcinka, jednak moim zdaniem ważna, to jest kwestia, no pewnej służby dla ojczyzny, którą można powiedzieć, że wyssałem z mlekiem matki, bo jestem z Gór Świętokrzyskich. Tam dosyć silna jest tradycja i pamięć o żołnierzach Armii Krajowej. I stąd pomysł wojska. Natomiast Wydział Cybernetyki to wydział, który ma długą historię. Właściwie to jest wydział, który prawdopodobnie, a moim zdaniem to prawdopodobieństwo jest równe 100%, był pierwszym wydziałem informatycznym w Polsce. Powstał w 1968 roku, nazwał się Wydziałem Cybernetyki, bo wówczas chodziło o wykorzystanie maszyn liczących do wsparcia dowodzenia, do wsparcia sterowania różnego rodzaju mniej lub bardziej złożonymi systemami, tym właśnie się zajęła cybernetyka. I ten wydział po prostu był i jest znany w Polsce właśnie z tego obszaru wsparcia dowodzenia, badań operacyjnych. I siłą rzeczy, ponieważ coraz bardziej wydajne mamy komputery, to tym więcej te komputery były w tym wsparciu wykorzystywane do przeprowadzania różnego rodzaju obliczeń. I po prostu to zaczęło mi się obijać o uszy, w latach 90' jak byłem w liceum, że jest taki Wydział Cybernetyki w Wojskowej Akademii Technicznej. I stąd pomysł na to, żeby tę informatykę studiować w wojsku. Może jeszcze powiem taką historyjkę, że Wydział Cybernetyki w pewnym momencie był pomysł, żeby zmieniać nazwę, ponieważ jak ktoś powiedział, że jest po Wydziale Cybernetyki, to nie bardzo było wiadomo, o co chodzi, co to jest za wydział.

Prowadzący: Nie do końca wiadomo, tak, tak.

Płk dr inż. Rafał Kasprzyk: Tak. I był pomysł, żeby zmienić na informatykę. Na szczęście ten pomysł się nie ziścił. I mamy Wydział Cybernetyki od 1968 roku, a słowo cyber teraz jest jak nigdy modne. I zajmujemy się cyberbezpieczeństwem i jak powiemy, że jesteśmy z Wydziału Cybernetyki, to, no to wiadomo, czym się zajmujemy mniej więcej.

Prowadzący: A jakie są Pana główne obszary zainteresowań, jeżeli chodzi właśnie o tematykę cyberbezpieczeństwa? Co jest tutaj tym konikiem?

Płk dr inż. Rafał Kasprzyk: Ja na ten, na ten obszar patrzę dosyć szeroko. Mianowicie, jak to cybernetyk, obszar sterowania złośliwego maszynami i ludźmi, bo tę cyberprzestrzeń można wykorzystywać właśnie do sterowania złośliwego na poziomie technicznym i tutaj mamy do czynienia z cyberatakami i przeciwdziałanie tego rodzaju akcjom. I na poziomie takim informacyjnym, że możemy próbować złośliwie sterować ludźmi poprzez dostarczanie albo niedostarczanie określonej informacji. I jakby to jest taki, taki mój, moje spojrzenie na ten obszar, czyli tak trochę z lotu ptaka, cyberprzestrzeń i kontekst zarówno maszyn mniej lub bardziej inteligentnych, ich podatności i ludzi, którzy też mają swoje podatności.

Prowadzący: Biorąc pod uwagę wiele w sumie Pana wypowiedzi znalezionych w sieci dotyczących tak naprawdę najróżniejszych ćwiczeń, badań czy konkursów przeprowadzanych dla studentów, nie mogę się oprzeć wrażeniu, że Pan bardzo mocno dopinguje swoich podopiecznych do kolejnych sukcesów. Co Pan sądzi o poziomie wiedzy i zaangażowania wychowanków WAT, jeżeli mogę tak to ująć?
[00:05:03]

Płk dr inż. Rafał Kasprzyk: Jak w każdym środowisku rozkład, rozkład jest pewien taki, można by powiedzieć dzwonowy. Natomiast mam takie wrażenie, że na Wydziale Cybernetyki ten dzwon, przez tego dzwonu przesuwa się w takim kierunku, no wskazującym, że mamy bardzo dobrych absolwentów, o może tak. Kończą wydział ludzie, którzy są na bardzo wysokim poziomie i to, mam za tym jakby dwa dowody. Pierwszy dowód taki biznesowy, że jak są prowadzone różnego rodzaju statystyki dotyczące zatrudnienia i zarobków absolwentów różnych uczelni politechnicznych w Polsce, to Wydział Cybernetyki, jakby jest w czołówce. Czyli, czyli nasi absolwenci mają kompetencje, za które to kompetencje biznes jest w stanie zapłacić. Drugi, drugi argument czy fakt potwierdzający, że, że mamy bardzo dobrych absolwentów to jest to, że rok rocznie bierzemy udział w różnego rodzaju maratonach , konkursach informatycznych, czy to krajowych czy międzynarodowych i jesteśmy bardzo często tę stroną czy tym graczem, który wygrywa albo w czołówce, co mnie bardzo cieszy.

Prowadzący: Panie Rafale, jak obecnie wyglądają możliwości kształcenia na kierunkach związanych z szeroko rozumianym cyberbezpieczeństwem, no właśnie na Wydziale Cybernetyki? Obecnie są to trzy Instytuty, tak? Jeżeli mógłby Pan przybliżyć ich profil, a także kierunki, które obecnie oferuje WAT?

Płk dr inż. Rafał Kasprzyk: Tak. Na Wydziale Cybernetyki mamy trzy Instytuty. Instytut Systemów Informatycznych to jest taki Instytut, który jakby mojemu sercu jest najbliższy, bo z tego Instytutu pochodzę. Jest Instytut Informatyki, Telekomunikacji i Cyberbezpieczeństwa oraz mamy Instytut Matematyki i Kryptologii. I te trzy Instytuty, no dzięki temu, że ich jest trzy to, to jak wiemy stół na trzech nogach jest bardzo stabilny, także my mamy kształcenie, dydaktykę bardzo stabilną i na wysokim poziomie, dzięki tym trzem Instytutom. Gdybym miał powiedzieć o kierunkach, jakie mamy na Wydziale Cybernetyki, no to przede wszystkim kierunek Informatyka oraz kierunek od 2016 roku Kryptologia i Cyberbezpieczeństwo. I tutaj znowu może tak nieskromnie, ale ten kierunek Kryptologia i Cyberbezpieczeństwo, to jest pierwszym tego rodzaju kierunkiem na uczelniach wyższych w Polsce. Na tych dwóch kierunkach kształcimy zarówno studentów cywilnych, jak i podchorążych, czyli kandydatów na żołnierzy zawodowych, którzy później zasilają korpusy osobowe, jak to się mówi w wojsku, korpusy osobowe właściwe łączności i informatyki, i kryptologii i cyberbezpieczeństwa. Można powiedzieć, że WAT w szczególności dzięki Wydziałowi Cybernetyki, ale również Wydziałowi Elektroniki, no jest takim rdzeniem dla tych dwóch korpusów żołnierzy zawodowych.

Prowadzący: Właśnie odnoszę wrażenie, że w Polsce następuje pewnego rodzaju przemiana. I to jest oczywiście również też w pewien sposób powiązane z Państwa jednostką tak, ale wiele osób związanych z cyberbezpieczeństwem powtarza troszeczkę jak mantrę słowa, że jest za mało specjalistów, a będzie tylko gorzej. Jakiś czas temu tak naprawdę rzeczywiście nie było raczej możliwości kształcenia się bezpośrednio na kierunkach związanych z cyberbezpieczeństwem, kryptologią i tak dalej. Ten trend się powoli zmienia. I czy jest to po prostu związane z zainteresowaniem tą tematyką czy ma na celu wypełnienie luk na wykwalifikowanych pracowników?

Płk dr inż. Rafał Kasprzyk: Moim zdaniem zainteresowanie taką tematyką techniczną jest dosyć stabilne. Natomiast zapotrzebowanie rośnie i będzie rosło, ponieważ jesteśmy otoczeni coraz bardziej przez zaawansowaną technologię. I być może coraz więcej osób chciałoby pójść na kierunki takie techniczne właśnie, dlatego że widać, że to jest przyszłość, rynek pracy taki pewny, stabilny. Natomiast wiadomo, w społeczeństwie mamy osoby, które są, urodziły się z różnymi zdolnościami. I tutaj tego po prostu nie zmienimy. Więc jakby trochę powtórzę, ale żeby powiedzieć zupełnie moje prywatne zdanie, że to zainteresowanie jest stałe od lat i będzie takie, prawdopodobnie.

[00:10:01]

Płk dr inż. Rafał Kasprzyk: Natomiast zapotrzebowanie będzie rosło. Nadzieja tutaj jest pewna w sztucznej inteligencji. I ta sztuczna inteligencja może nas w pewnym zakresie odciążyć od tego ogromu zadań, które przed nami, pozostawiając ludziom technicznym te części zadań, które wymagają już nie małpiej zręczności, tylko kreatywności.

Prowadzący: Panie Rafale, na uczelni był Pan kierownikiem wielu, wielu projektów. Czy mógłby Pan przybliżyć takie najciekawsze z Pańskiego punktu widzenia?

Płk dr inż. Rafał Kasprzyk: Taki, taki najciekawszy projekt z mojego punktu widzenia nie jest związany z cyber, ale może, ponieważ moim zdaniem jest najciekawszy, to go przybliżę. To jest taki projekt o akronimie CARE – Creative Application to Remedy Epidemics. I to jest projekt, który rozwijaliśmy ze studentami, potem doktorantami od 2009 roku w ramach konkursów, w szczególności Microsoft Imagine Cup. I tutaj chodziło o zbudowanie narzędzia, które będzie w stanie prognozować rozwój epidemii chorób zaraźliwych, czyli, czyli troszkę żeśmy wyprzedzili problem, z którym się mierzymy obecnie. I ten produkt, znaczy może ten, może tak powiem, ta koncepcja, później różnego rodzaju prototypy tego narzędzia były swego rodzaju takim paliwem dla różnych prac badawczych i magisterskich, pomysły na doktoraty tutaj wkoło tego się rodziły. A w końcu zbliżając się do tego, czym się zajmuje, to narzędzie do badania rozprzestrzeniania się wirusów takich biologicznych w jakimś stopniu od strony modelowej jest bardzo podobne do narzędzia, które może prognozować rozprzestrzenianie się różnego rodzaju wirusów komputerowych czy dezinformacji w sieci. I tutaj już jesteśmy bliżej tego, czego dotykamy w tym odcinku.

Prowadzący: W jednym z artykułów napisanych przez Pana, no trafiłem naprawdę bardzo ciekawe stwierdzenie i pozwolę sobie je przytoczyć, dobrze? „Sztuczna inteligencja nie dorówna ludzkiej, podobnie jak inteligencja ludzka nie sprosta sztucznej". W artykule opisuje Pan wachlarz tak naprawdę zagrożeń związanych z rozwojem nowoczesnych technologii, a także swoisty obraz wojny w przyszłości. Jak może wyglądać taka wojna? To już rozumiem niekoniecznie regularna armia i rakiety, a raczej komputery i infrastruktura?

Płk dr inż. Rafał Kasprzyk: Tak, właśnie z tym, z czym się mierzą siły zbrojne, czy w ogóle system bezpieczeństwa różnych państw, to jest ocena zmian środowiska bezpieczeństwa. Czyli musimy się zastanowić na poziomie tym najwyższym właściwie, na co my się szykujemy. Czy my się szykujemy na wojnę, która już była czy na wojnę, która przed nami, czy może właściwie na wojnę, która już jest. Bo jeśli chodzi o cyberbezpieczeństwo czy cyberprzestrzeń, to tutaj jest bardzo trudno odróżnić stan „p" od stanu „w", mówiąc wojskowo, czyli stan pokoju od stanu wojny. W takim klasycznym podejściu to wiemy po pierwsze, gdzie jest linia frontu, gdzie są obcy, gdzie jesteśmy my. Wiemy, czy mamy do czynienia z wojną, czy nie, bo najczęściej jedna strona wypowiada wojnę drugiej. Wiemy, gdzie mamy cywilów, wiemy, gdzie mamy żołnierzy, oni po prostu przebierają się, ci żołnierze w określone kolory. No i różnego rodzaju międzynarodowe prawa mówią, co można z żołnierzem, a co można, a czego nie można robić z cywilem, nawet w czasie wojny. Natomiast w cyberprzestrzeni zupełnie to wszystko się zaciera. Mamy taką magmę, lawę, która jest potężnym wyzwaniem i co więcej, teraz jakby wracając do tego artykułu, z którego Pan zacytował to takie moje przemyślenie, wydaje się, że te wojny w

przyszłości, to wojny na algorytmy. Przynajmniej, jeśli chodzi o wojny toczone w cyberprzestrzeni. To, czego po prostu my, jako ludzie nie jesteśmy w stanie osiągnąć, a maszyny mają to z automatu, to jest jakby prędkość, szybkość, przetwarzania olbrzymiej ilości danych. A właśnie wojna w cyberprzestrzeni to jest potrzeba przetwarzania olbrzymiej ilości danych, związanych z chociażby z rozpoznaniem, z tym, co robi przeciwnik, z targetowaniem, czyli wskazywaniem tego, co jest kluczowe dla przeciwnika, co należy w pierwszej kolejności zniszczyć, osłabić, aby tego przeciwnika pokonać.

[00:15:12]

Płk dr inż. Rafał Kasprzyk: No i reasumując, powtórzę, po prostu wojna przyszłości to prawdopodobnie wojny na algorytmy w cyberprzestrzeni i tym się między innymi na Wydziale Cybernetyki Wojskowej Akademii Technicznej zajmujemy.

Prowadzący: Wspomniał Pan właśnie przed chwileczką o wojnie na algorytmy. To jest kwestia stworzenia systemu, a po drugiej stronie stworzenia kontrofensywy, aby ten system nie działał? Jakby można było tutaj troszeczkę jeszcze bardziej rozwinąć koncepcję właśnie wojny na algorytmy.

Płk dr inż. Rafał Kasprzyk: Tak. To może króciutko o tej sztucznej inteligencji. Troszkę uproszczając, ale lubię to uproszczenie, bo ono oddaje istotę współczesnych metod, sposobów budowania inteligentnych maszyn. To pierwsza koncepcja, to jest taka, że jeśli chcemy zbudować inteligentną maszynę, która radzi sobie w jakimś kontekście, to w pierwszej kolejności my sami, jako ludzie musimy ten kontekst zrozumieć i opisać sposoby postępowania w tym kontekście, w tej dziedzinie, żeby poradzić sobie z wyzwaniem. Więc człowiek po prostu, który ma doświadczenie te reguły ma w głowie postępowania, żeby poradzić sobie z wyzwaniem, żeby wygrać. I te reguły z głowy tego eksperta przelewane są w postaci nilu bardziej zaawansowane, teraz upraszczam ifów , w różnym języku programowania do algorytmów, które są podstawą działania maszyny. I ta maszyna po prostu działa tak, jak my, jako ludzie tę maszynę żeśmy zaprogramowali. Więc musimy też przewidzieć różnego rodzaju możliwe, takie niestandardowe zdarzenia, z którymi maszyna musi sobie poradzić. A drugie podejście jest takie i ono jest coraz bardziej powszechne, ponieważ mamy niezwykle dużo danych, to my, jako ludzie, no nie jesteśmy w stanie tych danych przetworzyć. Za to mamy algorytmy uczenia maszynowego i to jest jeden podzbiór sztucznej inteligencji, które to algorytmy uczenia maszynowego są w stanie przetwarzać olbrzymie ilości danych i szukać w tych danych związków przyczynowo – skutkowych, a najczęściej to nawet nie związków przyczynowo –skutkowych, tylko różnego rodzaju korelacji. I teraz to współczesne podejście budowy inteligentnych maszyn to jest nasycanie algorytmu uczenia maszynowego olbrzymią ilością danych tak, aby ten algorytm nauczył się radzić sobie w określonej sytuacji. No na przykład rozpoznawać podejrzane obiekty na polu walki. I ostatecznie taki algorytm buduje, z tego algorytmu uczenia maszynowego buduje się pewien model radzenia sobie w określonej sytuacji. Ten model jest na tyle ostatecznie skomplikowany, że człowiek nie do końca

rozumie, dlaczego maszyna postępuje tak, a nie inaczej. A z drugiej strony okazuje się, że maszyna radzi sobie lepiej niż człowiek. W związku z tym powstaje maszyna, która świetnie sobie radzi w pewnej sytuacji, ale człowiek nie jest w stanie za bardzo ją oszukać no, bo nie wie jak ona działa. Żeby oszukać tę maszynę, niezwykle skomplikowaną, która działa według reguł nieznanych człowiekowi, musimy budować inny system, który uczy się tej maszyny i stara się znaleźć w tej maszynie właśnie podatności. No i tutaj dochodzimy właśnie do tych, do tej wojny na algorytmy i tu już niekoniecznie na algorytmy z obszaru kryptologii, kryptografia, kryptoanaliza, tylko praktycznie wojna software – software. I to ma swoją nazwę – Adversarial Machine Learning, takie antagonistyczne uczenie maszynowe. I wokół tego obecnie jest bardzo dużo prac prowadzonych w różnych ośrodkach, czy wojskowych czy cywilnych, w szczególności w Stanach NSA bardzo dużo poświęca czasu, jeśli chodzi o, i wysiłków, i pieniążków na badania wokół tego obszaru AML DARPA . No oczywiście również w Chinach dużo się dzieje, w Rosji i tak można by było mnożyć. W Polsce też różnego rodzaju badania są prowadzone.

Prowadzący: Do tego jeszcze na pewno chciałbym wrócić, ale skoro już Pan rozpoczął tę kwestię związaną ze sztuczną inteligencją i wykorzystaniem tejże inteligencji, to jeszcze raz chciałbym wrócić do tego artykułu, który pozwoliłem sobie zacytować wcześniej. Wspominał tam Pan również o możliwościach związanych właśnie z wykorzystaniem sztucznej inteligencji w militariach, w armii. I mówił Pan, że z jednej strony do stricte właśnie monitoringu to, o czym Pan też przed chwileczką powiedział, tak.

[00:20:03]

Prowadzący: I na przykład właśnie rozpoznawaniu, czy to stanu zdrowia czy różnych innych podejrzanych elementów, czy na przykład autonomiczne pojazdy, gdzie też oczywiście sztuczna inteligencja jest tutaj jak najbardziej potrzebna. Ale z kolei wspominał Pan o czymś takim, jak lethal autonomous weapon system. I czy te wizje nie wchodzą już troszeczkę tak właśnie na podwórko znane z hollywoodzkich filmów – „Raport mniejszości", „Terminator", czy to rzeczywiście przyszłość wojska?

Płk dr inż. Rafał Kasprzyk: Powiem tak, mam nadzieję, że to nie jest przyszłość wojska. Natomiast zdania są podzielone i w szczególności tu można by stosować czy próbować stosować teorię gier, bo najlepiej by było, gdybyśmy wszyscy się umówili, że nie będziemy tego rodzaju broni czy systemów uzbrojenia budować. Natomiast, no tak jak to w teorii gier z dylematu więźnia wynika, jeśli tylko jedna ze stron nie zastosuje się do tego, do tej umowy, która summa summarum, jeśli wszyscy będą przestrzegać jest najlepsza dla nas wszystkich, a tylko ta jedna właśnie się wyłamie, to wtedy ta jedna zyskuje przewagę. No, bo nie oszukujmy się, że to człowiek jest tym ogniwem, który opóźnia podjęcie decyzji. To powoduje z jednej strony oczywiście bardzo takie korzystne, korzystną sytuację, że no nie jesteśmy, a przynajmniej nie cały czas na granicy pokój – wojna. Nawet badania są takie prowadzone, że okazuje się, że gdybyśmy sztucznej inteligencji powierzyli decydowanie o tym, czy przechodzimy ze

stanu „p” do wojny, to sztuczna inteligencja by była dużo bardziej skora do tego typu działań tak, bo nie ma emocji i tego typu inteligentnych zachowań. Tam jest brutalna siła algorytmów. Jak się czyta amerykańskie raporty, to z tych amerykańskich raportów wynika, że niektóre strony są bardziej skore, żeby w tym kierunku pójść. No i się wskazuje, że właśnie Chińczycy czy Rosjanie są bardziej skorzy, żeby w tym kierunku pójść. Natomiast te takie autonomiczne czy półautonomiczne systemy uzbrojenia mogą się okazać w niektórych sytuacjach konieczne, żeby utrzymać przewagę. I wskazuje się dwie sytuacje. Pierwsza sytuacja jest taka, że maszyna znajduje się w obszarze, gdzie nie ma możliwości komunikacji, jest po, jakby poza zasięgiem. No i teoretycznie wówczas nie ma nad nią żadnego, żadnej kontroli. I jakby to jest jeden obszar, gdzie te takie autonomiczne, czy trochę lżej powiedzmy półautonomiczne systemy uzbrojenia śmiercionośne mogłyby się okazać potrzebne. Mam nadzieję, że tak nie będzie. A drugi obszar, to bym powiedział jeszcze bardziej taki science fiction, chociaż może też niekoniecznie, jeśli patrzymy na to, co się dzieje, chociażby dzięki NASK , to jest podbój kosmosu, gdzie właściwie te maszyny mogą znaleźć się czy znajdą się poza zasięgiem ludzi, a z kolei na takich obszarach, nad którymi chcielibyśmy w przyszłości mieć, o ile na to pozwolą możliwości przyszłej technologii, kontrolę. O, także tak bym może odpowiedział. Natomiast w wojsku, w Stanach Zjednoczonych, bo do tego najczęściej się odnoszę, ponieważ tam najwięcej materiałów jest jawnych, rozważa się takie trzy koncepcje, jeśli chodzi o sztuczną inteligencję i jakby nadzorowanie tej sztucznej inteligencji. Jedna koncepcja to jest taka, którą nazywamy human in the loop, czyli mamy taką, mamy sytuację, że żeby podjąć decyzję, to w tej pętli zawsze jest człowiek. Czyli maszyna wypracowywuje warianty działania, wcześniej analizuje dane, rekomenduje ten właściwy wariant według tej maszyny, a to człowiek ostatecznie podejmuje decyzje. I to jest Human in the loop. No i większość państw świata, no przyznaje się, że, czy stwierdza, że w tym kierunku idzie i ja mam nadzieję, że w tym kierunku będziemy szli. Poza tym, że mam nadzieję, że nigdy człowiek ostatecznie nie naciśnie tego przycisku „fire”, bo właściwie po to jest wojsko, żeby tego ognia nie było. Chociaż to może brzmi paradoksalnie. Druga koncepcja, to jest skrajnie odmienna – human out of the loop, czyli człowiek w ogóle poza tą pętlą decyzyjną.
[00:25:07]

Płk dr inż. Rafał Kasprzyk: No i tutaj faktycznie idziemy w takim kierunku science fiction, terminatorów, jakichś obiektów, które są całkowicie autonomiczne. No i chyba zbliżamy się do apokalipsy, tak. I trzecia koncepcja, to jest coś po środku – human on the loop, czyli człowiek jest poza pętlą, ale w każdym momencie może do tej pętli wejść i przerwać, przerwać działania tych autonomicznych systemów uzbrojenia.

Prowadzący: W jeszcze innej właśnie publikacji przedstawił Pan kolejną koncepcję, właśnie związaną z analizą, z gromadzeniem tych informacji, które mogą być przydatne przy tworzeniu późniejszym algorytmów i przy działaniu oczywiście tych systemów. Sztuczna inteligencja nas obserwuje, słyszy i

uczy się nas – czy tego chcemy czy nie. Jest to odniesienie do projektu, o którym Pan też tam wspominał, znawca bodajże, znawca Pentagonu tak, dotyczącego jak identyfikować osoby podejrzane o terroryzm, ten system do namierzania, rozpoznawania i śledzenia celu. Czy tego typu systemy są całkowicie bezpieczne dla dobrych obywateli, tak dobrych w cudzysłowie? Czy tego typu systemy, które powiedzmy analizują tak dużą ilość informacji o ludziach w nieodpowiednich rękach na przykład, czy po prostu w rękach napastnika, jeżeli dojdzie do jakichś kompromitacji tak, systemu, nie są zbyt dużym niebezpieczeństwem dla obywateli?

Płk dr inż. Rafał Kasprzyk: Moim zdaniem są. Paradoks polega na tym, że takie systemy istnieją i my się tym systemom poddajemy. Tylko w większości przypadków to są systemy nie państwowe, tylko to są systemy firm prywatnych, czyli Google, Facebook czy inne media społecznościowe. No wykorzystują tego rodzaju systemy, które przetwarzają olbrzymie ilości danych o nas samych i wypracowują nasze profile po to, żeby potem czerpać i załóżmy, że tylko po to, pieniądze z reklam, które nam są wyświetlane. Czyli takie systemy są, my się zgadzamy na to, żeby te systemy nas monitorowały i myślę, że od tego nie uciekniemy. Natomiast to musi być świadomość po prostu ludzi, którzy korzystają z cyberprzestrzeni czy z różnego rodzaju systemów w ramach tej cyberprzestrzeni, czyli w szczególności mediów społecznościowych, że Ci ludzie muszą wiedzieć, że po prostu są monitorowani i to niekoniecznie tam jest jakiś zły cel, tak. Natomiast dane o tych ludziach, o nas są gromadzone. Są rozwiązania na poziomie państwowym to, co się dzieje chociażby w Chinach. Jest taki system SCS, nie wiem czy ja teraz sobie przypomnę, chyba Social Credit Score, system oceny obywateli tak, który monitoruje dzięki bardzo rozwiniętej, dzięki bardzo rozwiniętemu systemowi kamer, tak. Tych kamer są miliony, nie wiem ile dokładnie, ale jakieś miliony w Chinach. Ten system spina to, co obywatel robi w cyberprzestrzeni z tym, co robi w świecie fizycznym. I każdy obywatel ma jakiś swój score, jakiś swój wynik. To jest też z jednej strony dla tych obywateli paradoksalnie bardzo atrakcyjne, bo wchodzi w obszar gry rywalizacja, a ludzie lubią grać, w szczególności młodzi. I jeśli grają cały czas to, to są tak nakręceni bardzo pozytywnie, chcą jak najwyższe te score uzyskiwać, te wyniki. Ale ostatecznie te wyniki, no nie wpływają tylko na to, jaki level gry ja osiągnę w świecie wirtualnym, ale wpływają na to, co ja mogę kupić, czego nie mogę kupić, jakie mieszkanie, w jakiej dzielnicy mogę kupić, czy się wpasowywuję w innych obywateli mieszkających w tej dzielnicy, czy nawet może dochodzić do tego, że w zależności od wyniku obywatel może wyjechać albo nie może wyjechać z Chin, tak. No i takie prace, nie tylko prace, no takie systemy po prostu powstają i to jest bardzo, bardzo niebezpieczne. I kończąc może ten wątek, znowu sobie coś przypomniałem, mam dużo wątków w głowie, jest taka książka o tym, gdzie, z tej książki, w tej książce było takie pytanie postawione – gdzie człowiek jest najbardziej, najbardziej taki otwarty, gdzie mówi prawdę? Czy policjantowi mówi prawdę, czy w sądzie

mówi prawdę, czy swojemu najbliższemu partnerowi mówi prawdę? I się okazuje, że to żaden z tych casów.

[00:30:05]

Płk dr inż. Rafał Kasprzyk: Prawdę mówimy najczęściej oknie przeglądarki, dokładnie w Google, tak. Przez to, jakie pytania zadajemy najwięcej możemy dowiedzieć się czy ta druga strona tak, te algorytmy najwięcej mogą dowiedzieć się o nas samych, tak. I to jest taki też paradoks, że my zadając pytania w Google, możemy zdradzić bardzo dużo informacji o nas samych, a w żaden inny sposób te informacje nie byłyby do pozyskania od nas, poza torturami okrutnymi.

Prowadzący: Panie Rafale, chciałbym jeszcze wrócić do kwestii takiego cyberkonfliktu, tak. Jakie jest prawdopodobieństwo wystąpienia właśnie takiego cyberkonfliktu na dużą skalę pomiędzy dwoma czy większą ilością państw? I jakie mamy możliwości biorąc pod uwagę Siły Zbrojne Rzeczypospolitej Polskiej na opór w tej materii?

Płk dr inż. Rafał Kasprzyk: Jakie jest prawdopodobieństwo na dużą skalę, to zależy troszkę od tego, trzeba by sobie odpowiedzieć, czy komukolwiek zależy na tym, żeby na dużą skalę taki konflikt wybuchł? Mam wrażenie, że na ten moment nikomu na tym nie zależy i w związku z tym do takiego konfliktu na dużą skalę nie dojdzie. Co innego by było, czy z inną sytuacją byśmy mieli do czynienia, gdyby jedna ze stron liczących się, jakby stanęła przed murem i nie miała nic innego, żadnej innej opcji, jak tylko blackout na taką skalę globalną. Natomiast mam nadzieję, że do takiej sytuacji nie dojdzie, czyli żadna ze stron nie zostanie postawiona przed takim ostatecznym krokiem. Analogicznie, jak to było w trakcie zimnej wojny i niewykorzystania na szczęście broni nuklearnej, tak. Natomiast na mniejszą skalę tego typu akcje w cyberprzestrzeni będą i właściwie są prowadzone, każdego dnia mamy z jakąś mniejszą lub większą, z mniejszym, większym cyberatakiem do czynienia. Teraz odpowiadając na drugie pytanie, czyli jak Siły Zbrojne Rzeczypospolitej Polskiej są przygotowane, to tak prosto mi ciężko powiedzieć, nawet gdybym w 100% był przekonany, jak to wygląda, to wtedy bym z kolei nie mógł powiedzieć tego. Natomiast z tego, co wiem i co mogę powiedzieć Siły Zbrojne posiadają zdolności do prowadzenia operacji w cyberprzestrzeni i ewidentnie te zdolności z roku na rok, a właściwie bym powiedział, że szybciej, z miesiąca na miesiąc są rozwijane do działań w cyberprzestrzeni, zarówno te takie zdolności indywidualne, czyli nasze, jako państwa, jak również my, jako państwo działamy w strukturach typu NATO czy Unia Europejska. No i w szczególności w NATO wypracowujemy mechanizmy współpracy, takie zdolności koalicyjne do działań w cyberprzestrzeni. No i one naprawdę, czy indywidualne czy te takie zdolności kolektywne w ramach NATO z miesiąca na miesiąc są podnoszone. Bardzo dużo w Polsce dzieje się od 2016 roku, kiedy mieliśmy do czynienia ze Szczytem NATO w Warszawie, gdzie podjęto właśnie decyzje o uznaniu cyberprzestrzeni, jako kolejnej domeny działań. Tak jak mamy domenę lądową, morską, powietrzną, tak również cyberprzestrzeń

została uznana, jako taka domena, pełnoprawna domena prowadzenia działań militarnych. No i wówczas siłą rzeczy we wszystkich państwach NATO i w NATO, jako całości podjęto bardzo duże, bardzo duży wysiłek, żeby sprostać temu wyzwaniu, ponieważ jeśli uznajemy jakąś przestrzeń za przestrzeń prowadzenia działań militarnych, no to są pewne konsekwencje, chociażby Artykuł 5 Traktatu Północnoatlantyckiego, który mówi, że po prostu agresja na jednego z członków NATO w danej, w domenie, akurat cyberprzestrzeń od 2016 roku jest uznawana, jako taki atak po prostu na państwo NATO, tak. No i tutaj, chociażby w Polsce były prowadzone prace nad koncepcją wojsk, które miałyby działać w cyberprzestrzeni. Skonsolidowano rozproszone zdolności Sił Zbrojnych zarówno, jeśli chodzi o takie zdolności stricte IT, jak i zdolności cyber w ramach Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, no i trwają prace nad budową struktur WOC – Wojsk Obrony Cyberprzestrzeni.

[00:35:05]

Płk dr inż. Rafał Kasprzyk: I tutaj bardzo kibicujemy, jako Wydział Cybernetyki i wspieramy, chociażby w ten sposób, że kształcimy podchorążych, którzy później zasilą Wojska Obrony Cyberprzestrzeni czy inne struktury, które są w tym momencie skonsolidowane w NCBC.

Prowadzący: Wspominał jeden z wcześniejszych odcinków, gdzie moim gościem był Mirosław Maj, który mówił wtedy wprost o aktorach tak, napędzanych przez różne państwa, konkretnych grupach, powiedzmy APT pracujących na zlecenia rządu, czy w wielu przypadkach, gdzie tak rzeczywiście naprawdę było więcej insynuacji powiedzmy, odnośnie źródła ataku niż dokładnych danych. I to też by się rzeczywiście ładnie spajało, że częściej mamy do czynienia z takimi bardziej rozmytymi, powiedzmy atakami, a niżeli takim otwartym konfliktem, prawda?

Płk dr inż. Rafał Kasprzyk: Tak, tak. No w cyberprzestrzeni przede wszystkim to, co jest charakterystyczne, to jest trudność tej atrybucji, czyli kto działa, kto jest tym aktorem, który wykonał pewną akcję. To nie mówię, że nie jest to niemożliwe, natomiast jest to dużo trudniejsze niż w świecie fizycznym. I to jest potężne wyzwanie, tak.

Prowadzący: Pytałem też o możliwości tak naprawdę wojskowe tak, Rzeczypospolitej Polskiej. Natomiast jeszcze chciałem się o jedną rzecz tutaj dopytać. Czy mówimy tylko i wyłącznie o Siłach Zbrojnych, czy również możemy, jako państwo liczyć na wsparcie, jak to się mówi takich wolnych strzelców, czyli osób, instytucji, które biorąc pod uwagę swoje doświadczenie i umiejętności są w stanie pomóc, ale nie są związane bezpośrednio z armią?

Płk dr inż. Rafał Kasprzyk: Tak. To jest świetny pomysł. I w ogóle ten pomysł jest adresowany przez kierownictwo NCBC, czy wyżej przez Ministerstwo Obrony Narodowej, żeby wykorzystać potencjał, jaki jest właśnie w tym systemie pozamilitarnym w Polsce, bo jest naprawdę potężny. My mamy informatyków czy specjalistów od cyberbezpieczeństwa na światowym poziomie, no i siłą rzeczy

większość z tych specjalistów jest poza armią. I dokładnie jest taki pomysł wykorzystania tych specjalistów, aby ci specjaliści wspierali obronę naszych systemów, a na wypadek wojny być może nawet jeszcze mocniej byli zaangażowani. No i tutaj jest kilka inicjatyw, chociażby powołanie komponentu cyber w ramach Wojsk Obrony Terytorialnej, czyli wśród tych ochotników, którzy się zgłaszają do Wojsk Obrony Terytorialnej. No jest taka specjalna grupa, bo to jest specjalna grupa absolwentów uczelni politechnicznych i różnych kierunkach, w szczególności informatycznych, ale również, no osób, którzy są specjalistami, a nie skończyli jakiejś uczelni wyższej. I oni są konsolidowani w ramach tego komponentu cyber w Wojskach Obrony Terytorialnej. Również są takie inicjatywy poza, poza monowskie powiedzmy, ale z pewnością z MON konsultowane, z fundacjami, które powstają. Na pewno wiem, że jest taka, to jest organizacja chyba mająca status fundacji – Polska Obywatelska Cyberobrona. Czyli taka struktura, która zupełnie poza MON działa, poza Siłami Zbrojnymi, ale idea jest taka, aby tę strukturę potencjalnie wykorzystać w przypadku wojny albo innych trudnych sytuacji, z którymi będziemy musieli się zmierzyć. Także tak, dokładnie takie pomysły są. I tutaj dużo się dzieje, żeby ten potencjał poza Siłami Zbrojnymi wykorzystać.

Prowadzący: Panie Rafale, jak wyglądają inicjatywy MON dotyczące takiego szeroko rozumianego cyberbezpieczeństwa? Oczywiście te, o których możemy tutaj otwarcie mówić, tak.

Płk dr inż. Rafał Kasprzyk: Tak, no bym powiedział, że spektrum tych działań jest bardzo, bardzo szerokie, co znowu niezwykle po prostu mnie cieszy, jako, jak się nazywam patriotę. I nie wszystkie oczywiście inicjatywy są medialne, nie wszystko słyszymy w mediach, bo po prostu nie o wszystkim można mówić. Ja również, jako tylko pracownik Wydziału Cybernetyki, a nie żołnierz, który, przynajmniej w tym momencie odpowiada za kierunki rozwoju Sił Zbrojnych, nie o wszystkim wiem. Natomiast to, o czym wiemy, to przede wszystkim można powiedzieć, że mamy program cyber, wspomniany program cyber.mil.pl i to jest taki bardzo szeroki projekt, program, mający na celu podnoszenie zdolności Sił Zbrojnych, a szerzej w ogóle całego systemu bezpieczeństwa naszego kraju na ataki w czy z cyberprzestrzeni. I czym się ten program charakteryzuje? No przede wszystkim charakteryzuje się tym, że kompleksowo do tematu udało się podejść. Po pierwsze można powiedzieć, że pierwszym filarem tego programu to jest konsolidacja, o czym wspomniałem rozproszonych kompetencji, zdolności poszczególnych jednostek Sił Zbrojnych, które działają w cyberprzestrzeni i jakby wynikiem tej konsolidacji jest właśnie Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni, które powstało, jako połączenie Narodowego Centrum Kryptologii i Inspektoratu Informatyki, i jakby to jest jeden obszar. No, a drugi obszar tego programu to jest po prostu takie systemowe wspieranie procesu budowy Wojsk Obrony Cyberprzestrzeni. No i tutaj w ramach tego systemowego wsparcia, przede wszystkim kładzie się nacisk na proces kształcenia, szkolenia tych absolwentów kierunków wojskowych, w szczególności Wojskowej Akademii Technicznej. Powstało WOLI – Wojskowe

Ogólnokształcące Liceum Informatyczne, też tutaj na terenie WAT, które jest potencjalnie też taką kuźnią potencjalnych absolwentów, czyli jest chęć, żeby absolwenci WOLI trafiali do Wojskowej Akademii Technicznej na kierunki typu Informatyka czy Kryptologia i Cyberbezpieczeństwo. Powstało w zeszłym roku Eksperckie Centrum Szkolenia Cyberbezpieczeństwa, które ma się zajmować i już się zajmuje szkoleniami już takimi specjalistycznymi. Poza tym z takich systemowych działań, moim zdaniem bardzo ważnych, to jest próba przynajmniej zasypania tej potężnej luki, jeśli chodzi o zarobki w biznesie, a w wojsku specjalistów z tego obszaru cyberbezpieczeństwa. No nie oszukujmy się, że po prostu te zarobki są, no bardzo wysokie w cywilu, no chociażby, dlatego że tych specjalistów brakuje. Wojsko ma pewne widełki i w te widełki po prostu trzeba się wpasować. Natomiast jednym z właśnie takich tutaj inicjatyw bardzo ważnych, to są stałe dodatki dla osób, które służą w korpusie osobowym informatyka czy w korpusie osobowym kryptologia i cyberbezpieczeństwo.

[00:45:09]

Płk dr inż. Rafał Kasprzyk: I to są dosyć znaczne też takie dodatki. No i mógłbym tak wymieniać. Po prostu tych działań na przestrzeni ostatnich kilku lat jest dużo. Wymieniam te, które i tak są znane medialnie, tylko próbuję je tutaj przedstawić w ramach jednej wypowiedzi.

Prowadzący: Panie Rafale, muszę poruszyć jeszcze aspekt związany z ćwiczeniami. Wspominał Pan o współpracy pomiędzy strukturami NATO i tutaj, po pierwsze wojskowe ćwiczenia „Zima 20". Ja przyznaję się, że nie mam zielonego pojęcia, no jak to wygląda i czy poszło dobrze, czy nie. Więc ja tylko bazuję tak naprawdę na kwestiach związanych z komentarzami, które się gdzieś tam później pojawiły, które nie były zbyt pochlebne. Ale znowuż z drugiej strony NATO Locked Shields 2021, gdzie polska drużyna dowodzona przez właśnie Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni, no zajęła czwarte miejsce. Więc, gratulacje. To pokazuje jak wysokie zdolności, chyba posiadamy po prostu w zakresie cyberochrony.

Płk dr inż. Rafał Kasprzyk: Tak, ćwiczeń w wojsku jest na różnych poziomach prowadzonych bardzo dużo i takich krajowych, i międzynarodowych. No i bym powiedział, że tutaj o dwóch tematach można rozmawiać. Można rozmawiać o stricte zdolnościach cyber i można rozmawiać o takich ćwiczeniach, które mają na celu zsynchronizować i efektywnie wykorzystywać zdolności z różnych domen. No i to, to ćwiczenie, o którym Pan wspomniał „Zima" to jest takie ćwiczenie, gdzie no nie ćwiczą cyber, tylko ćwiczą wojska, które...

Prowadzący: Tak.

Płk dr inż. Rafał Kasprzyk: Siły Zbrojne, które działają w różnych domenach, a cyber jest jakby taką domeną, która właściwie przecina wszystkie pozostałe, ponieważ jak cyber zawiedzie, no to chociażby możemy mieć problem z dostępnością poszczególnych usług, w szczególności z komunikacją. I o tych ćwiczeniach, takich stricte wojskowych to bym za dużo nie chciał mówić, żeby o czymś nie powiedzieć,

o czym nie powinienem mówić. Natomiast mogę powiedzieć króciutko o tych takich ćwiczeniach, gdzie ćwiczymy te zdolności cyber i one, te ćwiczenia mają jakby różną formę, mają taką formę, w której mierzymy się, zespoły z różnych państw się mierzą i zdobywają określone pozycje w rankingu. I takim ćwiczeniem jest to ćwiczenie, o którym Pan wspomniał Locked Shields, które to ćwiczenie jest organizowane przez Eksperckie Centrum w Tallinnie. To się nazywa NATO Cooperative Cyber Defence Centre of Excellence. I w tych, w tym ćwiczeniu od wielu, wielu lat Polska bierze udział i zwykle bardzo wysoko tutaj się pozycjonujemy. I to ćwiczenie właściwie ma na celu porównać się, porównać się przynajmniej w sytuacjach, które są potencjalnymi scenariuszami, przygotowanymi na potrzeby ćwiczeń. I jeszcze raz powiem tutaj, fajnie naprawdę, te pozycje są naprawdę wysokie. Z Wydziału Cybernetyki również bierzemy udział w tych ćwiczeniach. Są również takie ćwiczenia, które są organizowane przez Sojusznicze Dowództwo Transformacji NATO. W NATO mamy takie dwa najwyższe dowództwa strategiczne. I to jest dowództwo Allied Command Operations, to jest to dowództwo, które dowodzi operacjami prowadzonymi przez NATO. I takie dowództwo Allied Command Transformation, które to dowództwo jest odpowiedzialne za transformację w ogóle powiedziałbym, no dowództwa, czyli wskazywanie, w jakim kierunku należy się przetransformować, tak żeby zmierzyć się efektywnie z przyszłymi zagrożeniami. I to dowództwo, to ACT – Allied Command Transformation, chociażby organizuje takie ćwiczenia Cyber Coalition, gdzie próbujemy właśnie te zdolności cyber, nie tyle mierzyć się z innymi naszymi sojusznikami, tylko zgrywać te zdolności, żeby efektywnie uzyskiwać po prostu synergię zdolności działania w cyberprzestrzeni. Czy takie ćwiczenie CWIX. To jest ćwiczenie, teraz próbuję sobie przypomnieć – Coalition Warrior Interoperability eXcercise, eXamination, eXperimentation and eXploration.

[00:50:00]

Płk dr inż. Rafał Kasprzyk: I to ćwiczenie z kolei mniej się fokusuje na cyber, chociaż też, ale na silnie rozumiane IT i interoperacyjność tych systemów wykorzystywanych przez poszczególne państwa NATO. I my, jako Polska we wszystkich tych ćwiczeniach bierzemy aktywnie udział. No i oczywiście tu pierwsze skrzypce gra Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni.

Prowadzący: I słuchałem właśnie ostatnio na temat przebiegu Locked Shields i, no byłem pod wrażeniem jak, z jakim rozmachem tak naprawdę tego typu ćwiczenia są organizowane i jak tak naprawdę tego typu akcje mogą wyglądać.

Płk dr inż. Rafał Kasprzyk: Tu bardzo ciekawe jeszcze, może nie wspomniałem, że jeśli chodzi o ten Locked Shields, to tutaj się patrzy na te ćwiczenia w cyber na takim poziomie, który mi się bardzo podoba, czyli zarówno uwzględnia się działania takie stricte techniczne, jak i informacyjne. Czyli mamy do czynienia z operacjami CyberOps i InfoOps. Czyli wpływanie zarówno na systemy teleinformatyczne, jak i wpływanie na , czyli na ludzi, którzy w jakiś sposób są zaangażowani w konflikt.

Prowadzący: Moim i Państwa gościem był płk dr inż. Rafał Kasprzyk z Wydziału Cybernetyki Wojskowej Akademii Technicznej. Panie Rafale, jeszcze raz bardzo dziękuję za Pana obecność.

Płk dr inż. Rafał Kasprzyk: Bardzo, bardzo dziękuję Panie redaktorze. Bardzo dziękuję słuchaczom.

Prowadzący: Do usłyszenia w kolejnym odcinku.

Płk dr inż. Rafał Kasprzyk: Do usłyszenia.