Przegląd Bezpieczeństwa Wewnętrznego
2024, nr 31, s. 255–260

https://doi.org/10.4467/20801335PBW.24.025.20802

VARIA

# Debata „Globalne cyberbezpieczeństwo w obliczu nowej zimnej wojny"

SECURE 2024
Muzeum Historii Polski, 16 kwietnia 2024 r.

SYLWIA KŁOBUSZEWSKA

Autorka niezależna
https://orcid.org/0009-0005-4056-9626

W dniach 16–17 kwietnia 2024 r. Muzeum Historii Polski w Warszawie gościło uczestników 27. konferencji SECURE 2024 zorganizowanej przez NASK – Państwowy Instytut Badawczy i CERT Polska. Jest to najstarsza polska konferencja dotycząca cyberbezpieczeństwa, gromadząca cywilnych i wojskowych specjalistów w tej dziedzinie, a także m.in. twórców sztucznej inteligencji. W ramach tego spotkania odbyła się debata ekspercka pod hasłem „Globalne cyberbezpieczeństwo w obliczu nowej zimnej wojny". Jej moderatorem był Michał Baranowski – dyrektor warszawskiego biura German Marshall Fund, a do dyskusji zostali zaproszeni: prof. Aleksandra Gasztold z NASK oraz Katedry Bezpieczeństwa Wewnętrznego Uniwersytetu Warszawskiego, gen. dyw. Karol Molenda – Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni oraz płk Adam Ciszewski – zastępca szefa Agencji Bezpieczeństwa Wewnętrznego.

## Czy mamy do czynienia z cyberwojną?

Rozpoczynając debatę, Michał Baranowski nawiązał do artykułu z „The Economist", w którym sytuację w cyberprzestrzeni przedstawiono, w kontekście wojny w Ukrainie, jako równie ważną jak wojna na froncie fizycznym. Zadał pytanie, czy w obliczu aktualnych zagrożeń można już mówić o zimnej bądź prawdziwej wojnie w cyberprzestrzeni.

Odnosząc się do tego, gen. Karol Molenda stwierdził, że w cyberprzestrzeni bez wątpienia nie ma pokoju. W jego opinii dotychczas można było mówić o rywalizacji, aktualnie natomiast mamy do czynienia z konfliktem i „wyścigiem zbrojeń". Przeciwnicy doskonalą swoje umiejętności i tworzą narzędzia, wiedząc, gdzie jest próg wojny, i dbając o to, aby go nie przekroczyć. Nadmienił, że cyberprzestrzeń jest domeną operacyjną i (…) *musimy budować nasze kompetencje do wprowadzenia pełnego spektrum operacji w tej domenie na równi z innymi* (domenami – dop. S. K.)*: lądem, powietrzem, wodą, kosmosem*. Jego zdaniem aktualnie trwa (…) *rozpoznawanie siebie nawzajem, być może nawet implementowanie albo operacyjne przygotowanie środowiska – zdobywanie przyczółków, które w przyszłości można byłoby wykorzystać*. W tym kontekście jest to zimna wojna w cyberprzestrzeni. Wojnę zdefiniował natomiast jako (…) *moment, w którym efekty wykorzystywane w cyberprzestrzeni lub poprzez cyberprzestrzeń spowodują śmierć lub uszkodzenia infrastruktury krytycznej.* Jego zdaniem (…) *dopóki jednoznacznie nie powiązaliśmy skutków działań w cyberprzestrzeni ze zgonami czy trwałym zniszczeniem infrastruktury, to jesteśmy na etapie konfliktu*. Czy biorąc pod uwagę aktywność Rosji w Ukrainie, można mówić o pełnej wojnie nie tylko w świecie fizycznym, lecz także w cyberprzestrzeni? Generał Molenda zwrócił uwagę, że działania wojskowe, które są tam prowadzone, mają charakter wielodomenowy. Kiedy rosyjskie wojska przekraczały ukraińską granicę, jednocześnie w cyberprzestrzeni zaatakowano łączność satelitarną tego państwa. Ataki na infrastrukturę krytyczną i system energetyczny Ukrainy powodujące m.in. tzw. blackouty (nagłe, poważne awarie systemu elektroenergetycznego – dop. S. K.) miały wpływ nie tylko na funkcjonowanie tej infrastruktury (co odczuli również cywile), lecz także na przebieg misji wojskowej.

Kontynuując wątek zagrożeń w cyberprzestrzeni, ale z perspektywy służb specjalnych, płk Adam Ciszewski nawiązał do aktualnie wyjaśnianej sytuacji z użyciem w Polsce oprogramowania szpiegowskiego Pegasus. Przyznał, że (…) *z punktu widzenia służb specjalnych utrata informacji wrażliwych, kompromitujących m.in. polityków, osoby istotne dla funkcjonowania państwa, jest ogromną stratą, porównywalną do strat materialnych*. Podkreślił, że mając dostęp do internetu, można wskazać cel z każdego miejsca na świecie, a informacje pozyskane przez takie systemy mogą być przejęte i wykorzystane przez przeciwników, zwłaszcza tych, którzy

nie przestrzegają prawa i żadnych zasad. Zwrócił uwagę, że takie oprogramowanie jest w stanie tworzyć nie tylko Izrael. Odpowiadając na pytanie, czy w sytuacji przejścia od konfrontacji do konfliktu zasady powinny nadal obowiązywać, przypomniał o różnicach w działaniu służb wywiadowczych i kontrwywiadowczych. Te pierwsze łamią prawo państwa, w którym operują – te drugie muszą bronić praworządności. Z uwagi na to, że cyberprzestrzeń jest nieograniczona, również możliwości służb wywiadowczych są w niej większe, a zatem ta przestrzeń to dla nich bardzo atrakcyjna domena działań.

## Społeczny wymiar cyberzagrożeń

Jaką rolę odgrywa przygotowanie społeczeństwa na wyzwania związane z rozwojem nowych technologii i zmianami układu sił na świecie? Zdaniem prof. Aleksandry Gasztold układ liberalny obecnie chyli się ku upadkowi, a nowy porządek jeszcze nie został nazwany. *Czy będzie to ład, którego gra o rząd dusz będzie toczyła się w cyberprzestrzeni, trudno nam jeszcze powiedzieć. Lekcja wojny w Ukrainie, czy zostanie odrobiona, czy nie, o tym się przekonamy przede wszystkim w sferze społecznej* – stwierdziła. Przypomniała o doktrynie bezpieczeństwa informacyjnego powstałej w Federacji Rosyjskiej, zgodnie z którą wojna informacyjna jest prowadzona dwutorowo i obejmuje rozwiązania techniczne oraz aspekty psychologiczne. Zwróciła uwagę na potencjał społeczny Rosji w działaniach z zakresu odstraszania i obrony (są nim wyszkoleni aktywiści, jak również przestępcy) w sytuacji konfliktu czy wojny. Nadmieniła, że jest to lekcja do odrobienia przede wszystkim dla Polaków. Jako przykład kraju, który dobrze przygotowuje swoich obywateli do obrony cyberprzestrzeni, wskazała Estonię. Utworzono tam jednostkę cyberobrony, w której mogą działać ochotnicy. Zasugerowała, aby w sytuacji konfliktu wykorzystać tzw. Cyber Elfy oraz tworzyć, pod patronatem instytucji kontrwywiadowczych, wywiadowczych i wojskowych, bazy osób działających na pograniczu cyberbezpieczeństwa i cyberataku. Organizowanie cyberrezerw powinno obejmować również szkolenie społeczeństwa na wypadek ataków nie tylko tych przeprowadzanych za pomocą szkodliwego oprogramowania, lecz także tych o charakterze psychologicznym.

Do potrzeby odpowiedniego przygotowania społeczeństwa na ataki cybernetyczne odniósł się również gen. Molenda. Przypomniał, że w Polsce poza służbami czy Dowództwem Komponentu Wojsk Obrony Cyberprzestrzeni funkcjonują Wojska Obrony Terytorialnej, w ramach których istnieje cyberkomponent. Podkreślił ważną rolę szkoleń Locked Shields (największe i najbardziej złożone ćwiczenia z zakresu cyberbezpieczeństwa organizowane przez NATO – dop. S. K.), dzięki którym tworzy się elitę ekspertów mogących zapewnić wsparcie w sytuacji wojny

w cyberprzestrzeni. Generał zaznaczył, że jest wiele do zrobienia w kwestii walki z dezinformacją. Nie jest to łatwe, gdyż instytucje są zobowiązane działać na podstawie i w granicach prawa, a przeciwnik posługuje się metodami dalekimi od zasad praworządności. Jego zdaniem pomocne w przeciwdziałaniu dezinformacji mogą być organizacje pozarządowe, a także takie inicjatywy, jakie podejmuje NASK.

## Konflikty w cyberprzestrzeni – wizja przyszłości

Następnym punktem debaty była próba odpowiedzi na pytanie, jak w przyszłości będą wyglądały konfrontacje czy wojny w cyberprzestrzeni.

Według płk. Ciszewskiego, mówiąc o przyszłości, musimy jednocześnie pamiętać o tym, jaką drogę przeszliśmy. Ważne było utworzenie Narodowego Centrum Kryptologii (NCK) – podmiotu dbającego o potencjał tej dziedziny. Nadmienił, że (…) *było to pewne wizjonerstwo wynikające z potrzeb, które wówczas mieliśmy jako służby, a dotyczące deficytów w zakresie kryptografii nie w kontekście ówczesnej sytuacji, tylko w kontekście przyszłości*. Odnosząc się do problemów służb mogących rzutować na ich funkcjonowanie w przyszłości, zasygnalizował trudności z rekrutacją profesjonalnych kadr. W jego opinii (…) *na chwilę obecną ustawą o obronie Ojczyzny całkowicie zamknięto możliwość zasilania służb cywilnych absolwentami uczelni wojskowych o specjalizacjach nam niezbędnych, podczas gdy dalej jesteśmy komponentem państwowym*. Jego zdaniem nie wykorzystuje się w pełni potencjału tych służb. Pułkownik Ciszewski zwrócił również uwagę na problem z ochroną łączności rządowej. Aktualnie bowiem zbyt wiele podmiotów zajmuje się tym tematem, co powoduje jego rozproszenie. Wskazał także na niebezpieczeństwa wynikające z łączenia przez funkcjonariuszy publicznych dwóch obiegów informacji – tych przekazywanych kanałami zamkniętymi oraz za pośrednictwem internetu. To może prowadzić do wycieków informacji. Podkreślił, że trwają analizy w tej materii, aby poprawić bezpieczeństwo łączności rządowej.

Według prof. Gasztold w badaniach nad cyberbezpieczeństwem najczęściej mówi się o trzech możliwych scenariuszach przyszłości – entuzjastycznym, który Polska powinna odrzucić m.in. z uwagi na problemy związane z bezpieczną łącznością, pragmatycznym, z którym aktualnie mamy do czynienia w większości konfliktów zbrojnych, oraz zaprzeczającym. Istotny wpływ na przebieg konfliktu może mieć odpowiednie wykorzystanie nowych technologii, w tym sztucznej inteligencji. Według prof. Gasztold (…) *drony czy oprogramowania wykorzystujące sztuczną inteligencję nie są srebrną kulą na wilkołaki. Oprogramowania te* (…) *mogą wzmocnić, posługując się terminem z Clausewitza, Nebel des Krieges, czyli mgłę wojny, i przeciwdziałać dezinformacji czy też wojnie psychologicznej*. Podkreśliła, że konflikt

rosyjsko-ukraiński jest lekcją dla sojuszników Ukrainy, którzy wyciągną wnioski dla swoich systemów obronnych. Jej zdaniem obecnie problem stanowi nie broń atomowa, lecz cyberprzestrzeń, a w przyszłości również sfera kosmiczna. Stwierdziła: (…) *nie można porównywać zastosowania broni jądrowej ze zmasowanymi operacjami w cyberprzestrzeni, które oddziaływają nie tylko na elity polityczne, instytucje bezpieczeństwa, ale na całe społeczeństwa czy też diaspory tych społeczeństw rozproszone w ujęciu globalnym*. Trudno jest zatem mówić o możliwości odniesienia pełnego zwycięstwa w tej przestrzeni. Według prof. Gasztold strategia odstraszania powinna zakładać pewne straty. Jakiego rodzaju one będą i w jakiej skali, to zależy od danego państwa.

Wątek konfliktów przyszłości kontynuował gen. Molenda. Podobnie jak płk Ciszewski nawiązał do utworzenia NCK. W kontekście powstania Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni (utworzonego na bazie NCK – dop. S. K.) stwierdził, że połączenie NCK oraz Inspektoratu Informatyki było dobrą decyzją. Dzięki temu powiązano bezpieczeństwo z funkcjonalnością. Podkreślił wagę współpracy tych dwóch oddzielnych „organizmów", potrzebnej zwłaszcza w przypadku zaistnienia incydentów krytycznych. Odwołując się do przykładu Ukrainy, zwrócił uwagę na udział obywateli dostarczających informacje siłom zbrojnym, jak również na problematykę ochrony informacji niejawnych w tym kontekście. Wyzwania na przyszłość wiążą się, jego zdaniem, nie tylko z wykorzystaniem sztucznej inteligencji podczas wojny, lecz także z udziałem w niej całego kraju, wraz z obywatelami i instytucjami, oraz z potrzebą, aby te wszystkie elementy działały interoperacyjnie. W związku z tym siły zbrojne muszą inaczej programować swoje systemy.

W kontekście udziału w wojnie cywili, włączanych w systemy współpracy w sferze cyber i konfrontacji fizycznej, padło pytanie od publiczności dotyczące kwestii ich ochrony, z uwagi na to, że nie mają oni takiego statusu jak żołnierze. Odnosząc się do tego, prof. Gasztold stwierdziła, że władza należy do tych, którzy mają wiedzę, odpowiedzią zatem jest edukacja jako sposób na kształtowanie aktywnego, świadomego cyberobywatelstwa. Edukować należy różne grupy społeczne, zaczynając już od najmłodszych (chociażby na temat urządzeń, z których korzystają), i promować wiedzę o zagrożeniach, a także obserwować trendy społeczne. Ważną rolę do odegrania mają tu instytucje takie jak NASK oraz instytucje pożytku społecznego. Potrzebne jest również stworzenie platformy czy też centrum wiedzy o zagrożeniach.

Odnosząc się do pytania o aktualne priorytety w kontekście cyberbezpieczeństwa, płk Ciszewski zgodził się z wypowiedzią prof. Gasztold dotyczącą roli edukacji oraz ponownie wskazał na problem łączności. O przestrzeń informacyjną zadbamy, gdy zapewnimy dobre, bezpieczne kanały łączności. Nawiązał także do

tego, o czym wcześniej mówił gen. Molenda na temat informacji niejawnych. Jego zdaniem należałoby podjąć dyskusję o ich ochronie i wypracować nowe podejście do tej problematyki.

Z wnioskami przedmówców zgodził się gen. Molenda, podnosząc raz jeszcze rolę edukacji. Problemem jest (…) *bezrefleksyjne wykorzystywanie nowej technologii zwłaszcza wśród młodzieży, bez wiedzy na temat zagrożeń* – stwierdził. Podkreślił również, że w przyszłości zwycięstwo będzie zależało od umiejętności współpracy różnych zespołów i integrowania ich działań, w ramach których ważne będą kreatywność i innowacyjność w poszukiwaniu nowych rozwiązań. Współpraca oznacza według niego najwyższy poziom zaufania między współdziałającymi zespołami, gdy wszyscy są świadomi, że priorytetem jest osiągnięcie wspólnego celu.

Sylwia Kłobuszewska

Autorka niezależna.