European Repository of Cyber Incidents

Z niewielką pomocą moich przyjaciół? Pomoc cybernetyczna i skuteczna cyberobrona Ukrainy

Martin Müller, Uniwersytet w Innsbrucku
Sebastian Harnisch, Uniwersytet w Heidelbergu
Tłumaczenie polskie: Joanna Kulesza, Uniwersytet Łódzki

Po upływie roku od rozpoczęcia działań wojennych na Ukrainie, jasne stało się, że dostęp do informacji wywiadu i zastosowanie rozwiązań cybernetycznych wpływa na sukces konwencjonalnych operacji wojskowych jedynie w umiarkowany sposób. Przykłady można mnożyć: we wczesnych fazach wojny CERT-UA był w stanie złagodzić wpływ szkodliwego oprogramowania "Caddy Wiper/Industroyer2" i jemu podobnych programów dzięki współpracy ze służbami wywiadowczymi innych państw (np. Wielkiej Brytanii, USA i Polski) oraz z firmami zajmującymi się cyberbezpieczeństwem, takimi jak ESET i Microsoft. Niedawno pojawiły się publicznie doniesienia o "ofensywnych operacjach cybernetycznych" prowadzonych przez władze USA, choć ich szczegóły (czas, miejsce i środki) nie są jeszcze znane.

Udzielanie (cyber)pomocy Ukrainie wywołało w wielu państwach obawy dotyczące ich ewentualnej odpowiedzialności międzynarodowej jako stron walczących, biorących udział w działaniach wojennych, tak jak np. w Niemczech (zobacz tu, tu i tu). Podzielając niektóre z tych obaw, dotyczących samej pomocy cybernetycznej dla Ukrainy jako mogącej prowadzić do eskalacji konfliktu, nie zgadzamy się z podobną oceną jej skutków. Z politycznego punktu widzenia operacje cybernetyczne mają wpływ na dostęp do informacji lub treści, przy czym bardzo niewiele operacji wywołuje efekty kinetyczne. W związku z tym pomoc cybernetyczna może prowadzić wręcz do deeskalacji konfliktu, o ile ma miejsce przed, w trakcie lub pod koniec działań wojennych. Jednocześnie odnotowujemy, że z punktu widzenia norm prawa międzynarodowego atak Rosji na Ukrainę jest bezprawnym użyciem siły, napaścią zbrojną z bezpośrednim i wyraźnym naruszeniem Karty Narodów Zjednoczonych.

Atak taki, naszym zdaniem, pozwala na dwie zgodne z prawem reakcje w cyberprzestrzeni: po pierwsze, zaatakowana strona, Ukraina, może bronić się indywidualnie lub zbiorowo na podstawie art. 51 Karty Narodów Zjednoczonych; po drugie, takie (niesprowokowane) użycie siły zbrojnej daje państwom możliwość albo powstrzymania się od udziału w działaniach zbrojnych, oferując jedynie wsparcie państwom realizującym swoje prawo do indywidualnej samoobrony zgodnie z art. 51 ust. 2 Karty Narodów Zjednoczonych albo wzięcia współudziału w walce, w której to państwo zaatakowane uczestniczy (jak tu i tu).

Podczas gdy dyskusja na temat (cyber)pomocy Ukrainie toczy się już od jakiegoś czasu (porównaj tu i bardziej szczegółowo tu), dyskusja ta, naszym zdaniem, nie objęła bezpośrednio kwestii tego, czy ulegająca zmianom praktyka państw w pierwszym roku działań wojennych już przesunęła granicę między niepodejmowaniem działań zbrojnych w cyberprzestrzeni a współudziałem w takich działaniach.

W tym krótkim artykule odpowiadamy na to pytanie. W pierwszej kolejności omawiamy międzynarodowe zobowiązania prawne podmiotów państwowych i niepaństwowych, pomagających Ukrainie w cyberprzestrzeni i zastanawiamy się nad ich działaniami i zaniechaniami. Dochodzimy do wniosku, że chociaż wydawać by się mogło, iż ofensywne operacje cybernetyczne były prowadzone przez władze Ukrainy i USA, nie były one równoznaczne z "użyciem siły", a więc z udziałem pomagającej strony trzeciej w walce, czyniąc ją stroną międzynarodowego konfliktu zbrojnego. W zaleceniach politycznych nakreślimy granice, które państwa powinny wziąć pod uwagę, wspierając cyberobronę Ukrainy.

Operacje cybernetyczne wspierające Ukrainę: między powstrzymywaniem się od działań zbrojnych a pomocą stronie walczącej

Warunki, po spełnieniu których państwa stają się bezpośrednimi stronami działań wojennych, mają kluczowe znaczenie dla stosowania międzynarodowego prawa humanitarnego (MPH), opisywanego przez konwencje genewskie. Jednak okoliczności, które sprawiają, że państwo staje się stroną międzynarodowego konfliktu zbrojnego, uległy istotnym zmianom na przestrzeni lat. Współczesne rozumienie, opisane szczegółowo tu (s. 7-15), zakłada, że udział w toczącym się konflikcie zbrojnym wymaga "bezpośredniego powiązania operacyjnego, zmierzającego do wyrządzenia szkody przeciwnikowi" w połączeniu ze „swojego rodzaju koordynacją" między państwem wspierającym i wspieranym.

W oparciu o te dwa kryteria dowodzimy, że zapewnienie pomocy operacyjnej lub udostępnienie informacji wywiadu na potrzeby obrony przed cyberatakami nie może uczynić państwa stroną konfliktu. Po pierwsze, operacjom tym regularnie brakuje "operacyjnego ogniwa szkodzenia przeciwnikowi", ponieważ albo nie szkodzą bezpośrednio atakującemu, tj. jedynie wspomagają wysiłki strony broniącej się w działaniach wojennych, i/lub zapobiegają uzyskaniu korzyści przez atakującego. Jako takie, działania te pozbawione są charakteru bojowego, ponieważ państwo udzielające pomocy nie stosuje środków, które osiągają poziom użycia "siły zbrojnej", ani nie są podejmowane celowo, niezależnie i z bezpośrednim zamiarem zaszkodzenia przeciwnikowi.

Podczas działań wojennych na Ukrainie do tej pory żadne państwo udzielające pomocy nie zgłosiło oferowanego wsparcia Radzie Bezpieczeństwa ONZ, jak wymaga tego art. 51 ust. 2 Karty Narodów Zjednoczonych względem państw współuczestniczących w konflikcie zbrojnym, zatem naszym zdaniem praktyka państwa udzielającego takiej (cyber)pomocy stworzyła swoistą szarą strefę "niedeklarowanej nieinterwencji" w cyberprzestrzeni. Rosyjskie władze sygnalizują, że niektóre operacje cybernetyczne, np. skutkujące odłączeniem satelity zwiadowczego, będą przez nie odczytywane jako równoznaczne z atakiem zbrojnym. Na razie jednak możemy wstępnie stwierdzić, że państwowa praktyka "niezadeklarowanego udziału w cyberwojniej" podczas działań wojennych jest bezsporna. Wynika z tego, że środki podejmowane przez różne państwa mające na celu zapobieganie cyberatakom na Ukrainie – wysyłanie własnego personelu ds. cyberbezpieczeństwa, szkolenie personelu zagranicznego lub dostarczanie "dostosowanych" rozwiązań w zakresie oprogramowania zabezpieczającego w celu ochrony systemów informatycznych lub, po rozpoczęciu działań wojennych, wykrywanie napastników w spenetrowanych systemach i uniemożliwianie im dalszych działań – są legalną praktyką państwową w ramach tego "niezgłoszonego statusu".

A przecież państwa udzielające pomocy mogą stać się stronami w międzynarodowym konflikcie zbrojnym, jeśli przekroczą granicę pomiędzy pomocą w samoobronie indywidualnej Ukrainy a jej zbiorową samoobroną w ramach (ogłoszonej) koalicji państw zgodnie z art. 51 KNZ. Ten ostatni status nadal byłby uzasadnioną odpowiedzią na akt agresji ze strony Rosji,zgodnie z normą opisaną w art. 21 Artykułów o odpowiedzialności państwa Komisji Prawa Międzynarodowego, zwłaszcza gdyby został zgłoszony Radzie Bezpieczeństwa ONZ. Współdziałanie uruchomiłoby jednak zasady prawa wojny (międzynarodowego prawa humanitarnego, MPH), a tym samym pozwoliłoby na zainicjowanie przez Rosję (choć bezpodstawnie, bowiem ma ona tu status agresora) środków zaradczych wobec członków tak skonstruowanej koalicji obronnej (takie środki zaradcze oczywiście nadal musiałyby

spełniać wymogi MPH, tj. m.in. uczynić zadość zasadzie proporcjonalności). Prawdopodobnie rodzaj ofensywnych operacji cybernetycznych, np. powstrzymanie ataku poprzez (tymczasowe) wyłączenie (rosyjskiego) serwera, dostarczenie danych wywiadowczych lub wywoływanie bezpośredniego wpływu na działania atakującego, może, ale nie musi, przekraczać próg bezpośredniego udziału w działaniach wojennych, również w zależności od interpretacji tego, czy środki zostały podjęte w celu użycia siły zbrojnej (listę stanowisk państw w tej kwestii można znaleźć tu).

Po dziś dzień jednak ani państwa pomagające Ukrainie nie nabyły statusu współwalczących, deklarując swój udział w zbiorowej samoobronie wobec Rady Bezpieczeństwa ONZ, ani operacje ofensywne (rzekomo) podejmowane przez USA nie zostały zinterpretowane i uznane przez władze rosyjskie jako "użycie siły zbrojnej". Jednak doniesienia o wymianie informacji wywiadowczych posiadanych przez Stany Zjednoczone na temat dokładnej geolokalizacji zasobów wojskowych (np. niszczyciela Moskwa) i personelu (np. wyższych oficerów rosyjskich) wywołały dyskusję polityczno-prawną na temat kryteriów, które uznać należy za determinujące status państwa jako zaangażowanego w trwający międzynarodowy konflikt zbrojny (por. tu, tu i tu). Ponadto przy różnych okazjach rosyjscy urzędnicy grozili, że uznają komercyjne systemy satelitarne za uzasadnione cele, jeśli zostaną wykorzystane do "celów wojskowych".

Zgodnie z obowiązującymi normami międzynarodowymi dotyczącymi udziału w działaniach zbrojnych uznajemy, że przy kwalifikacji prawnej wymiany informacji wywiadu należy wziąć pod uwagę co najmniej dwa elementy. Po pierwsze, wymiana takich informacji może być niezgodna z prawem, ponieważ państwo dzielące się informacjami mogło je pozyskać niezgodnie z prawem, na przykład poprzez stosowanie tortur, co jest zabronione przez normy peremptoryjne, lub mogły zostać pozyskane z naruszeniem suwerenności innego państwa, na przykład poprzez dokonanie ataków cybernetycznych, nie mających uzasadnienie w prawie do międzynarodowym. Po drugie, wymiana informacji wywiadu może stanowić podstawę uznania za bezprawne działania państwa je przyjmującego. W obu przypadkach istotny może okazać się współudział określony w art. 16 Artkułów o odpowiedzialności państwa KPM i powiązanych z nimi normach prawnych (por. szczegółowo s. 1385 i nast.).

Biorąc pod uwagę brak rosyjskich działań prawnych lub bezpośrednich działań kinetycznych przeciwko Stanom Zjednoczonym jako państwu dzielącemu się danymi wywiadowczymi oraz ograniczony skutek wymiany informacji wywiadowczych w porównaniu z operacjami sił konwencjonalnych wspomaganych cybernetycznie, dochodzimy do wniosku, że wymiana informacji wywiadowczych niesie ze sobą znacznie większe ryzyko wciągnięcia strony trzeciej do konfliktu zbrojnego niż

jakiekolwiek "ofensywne operacje cybernetyczne". Wynika to z faktu, że koszty skutecznego zintegrowania ofensywnych operacji cybernetycznych z konwencjonalnymi działaniami wojskowymi lub skutecznego prowadzenia ofensywnych operacji cybernetycznych, które sprowadzają się do "użycia siły", pozostają (bardzo) wysokie, a zyski z zastosowania niezgodnych z prawem, ofensywnych działań cybernetycznych, np. wpływania na działanie elektrowni jądrowej lub ataku na szpital, pozostają niskie.

Podmioty niepaństwowe i operacje cybernetyczne podczas działań wojennych w Ukrainie

Od 24 lutego 2022 r. podmioty niepaństwowe wymieniają się informacjami wywiadowczymi i prowadzą operacje cybernetyczne. Do tej pory jednak czyny te nie osiągnęły poziomu "użycia siły" czy "zbrojnej napaści". Zamiast tego zdecydowana większość operacji była "głośna i krótka", obejmując ataki DDoS, ingerencję w spójność danych i nieuprawniony dostęp do nich. Analizując rodzaje pomocy cybernetycznej dla Ukrainy, można wyróżnić trzy grupy podmiotów w nią zaangażowanych: jednostki i grupy, które działają niezależnie od władz ukraińskich; jednostki i grupy, które zorganizowały się w "Informatyczną Armię Ukrainy" oraz prywatne podmioty, które w większości przypadków mają (i miały przed rozpoczęciem wojny) stosunki umowne z rządem Ukrainy lub innymi rządami w celu wspierania interesów ukraińskich. Te podmioty niepaństwowe można odróżnić od organów państwowych, takich jak CERT-UA, który jest częścią "Państwowej Służby Specjalnej Komunikacji i Ochrony Informacji". Działania tych podmiotów mogą być przypisane Ukrainie na mocy prawa międzynarodowego jako organom państwa zgodnie z art. 4 Statutu Odpowiedzialności Państwa.

Jeśli chodzi o pierwszą grupę niezależnych aktorów, różne grupy haktywistów, takie jak Anonymous, GNG, NB65, Ghostsec i Cyber Partisans, wypowiedziały "cyberwojnę Rosji" lub włączyły się w operacje cybernetyczne przeciwko rosyjskim interesom.

Choć niektóre z tych operacji noszą znamiona pośredniego udziału w działaniach wojennych, przy braku szkód militarnych i koordynacji w stopniu odpowiadającym bezpośredniemu udziałowi stron wspierających Ukrainę, nie wywołały jak dotąd prawnej ani politycznej kontrreakcji władz rosyjskich. Rosja nie podjęła również działań zmierzających do pociągnięcia do odpowiedzialności poszczególnych państw, z terytoriów których podmioty te operują, nawet jeśli miejsce ich działania jest znane, przywołując naruszenie zasady należytej staranności (interpretacja związana z cyberprzestrzenią, s. 30 i nast. oraz tutaj). Ponadto, według naszej wiedzy, władze rosyjskie nie próbowały współpracować z innymi państwami lub organizacjami międzynarodowymi (np. Interpolem) w celu pociągnięcia tych osób do

odpowiedzialności za cyberprzestępstwa w znaczeniu rosyjskiego kodeksu karnego. W związku z tym, w obliczu licznych (choć nieregularnych) operacje cybernetyczne prowadzonych przez niezależne podmioty niepaństwowe podczas działań wojennych na Ukrainie, rząd Rosji wolał milczeć z prawnego punktu widzenia.

Drugą grupę podmiotów, w szczególności reprezentowana przez "IT Army of Ukraine", można nazwać swego rodzaju "cybernajemnikami", ponieważ ich cel, sposób działania i łańcuch operacyjny sięgają ukraińskiego rządu, tj. Ministerstwa Transformacji Cyfrowej, wzywającego do międzynarodowego wsparcia obrony Ukrainy. Biorące w nich udział osoby i grupy (w pewnym momencie doniesienia prasowe mówiły o 300 000 ochotników) uczestniczą w defensywnych i ofensywnych operacjach cybernetycznych. Z prawnego punktu widzenia można ich zatem zaklasyfikować jako ludność cywilną bezpośrednio lub pośrednio wspierającą działania wojenne. Pierwsza kategoria miałaby zastosowanie do osób, które celowo angażują się w operacje cybernetyczne w celu wywarcia negatywnego wpływu na operacje wojskowe lub zdolności wojskowe rosyjskich sił zbrojnych, co skutkuje bezpośrednimi powiązaniami przyczynowymi między działaniami a szkodami po stronie Rosji na korzyść Ukrainy. Z tego co wiemy, władze rosyjskie nie zwracały się otwarcie, ani w formule prawnej ani politycznej, do członków tych grup indywidualnie lub zbiorowo jako do uczestników IT Army of Ukraine. Z kolei rosyjskie władze twierdzą, że "żaden z najemników, których Zachód wysyła na Ukrainę, by walczyli po stronie nacjonalistycznego reżimu w Kijowie, nie może być uznany za stronę walczącą zgodnie z międzynarodowym prawem humanitarnym ani nie może mieć statusu jeńca wojennego".

Trzecia grupa podmiotów obejmuje szeroki wachlarz firm: sa to zarówno duże, głównie amerykańskie platformy informatyczne, takie jak Microsoft i Google, jak i małe, wyspecjalizowane firmy zajmujące się cyberbezpieczeństwem. Rzekomo firmy te odegrały kluczową rolę w "ewakuacji" ważnych danych ukraińskiego rządu do usług w chmurze na przełomie lutego i marca 2022 r. i ochronie ich, zapewniając jednocześnie bezpieczeństwo sieci dostępnej dla ukraińskich instytucji rządowych i sieci publicznych oferując analizę zagrożeń, wykrywanie i działania obronne.

Rzekomo niektóre z tych firm ściśle współpracowały z władzami USA i Ukrainy, mimo że w odniesieniu do większości takich usług nie istniała znana podstawa umowna takiej współpracy (por. tu i tu). Analizując zasady odpowiedzialności państwa w prawie międzynarodowym, można by rozważyć przypisanie jej Ukrainie lub USA na podstawie art. 8 Artykułów (działanie kierowane lub kontrolowane przez państwo), ale analiza taka byłaby błędna, bowiem nie ma dowodów na to, że wpływ rządów USA lub Ukrainy był wystarczająco duży, aby osiągnąć wymagany tym przepisem próg kontroli lub wpływu. Co więcej, w ramach "Cybersecurity Tech Accord" ponad 100

wiodących firm zajmujących się bezpieczeństwem IT zobowiązało się nie wspierać cyberataków ze strony rządów. Oprócz "cybernajemników" nie zaobserwowaliśmy w tym momencie żadnych rosyjskich działań przeciwko firmom zajmującym się bezpieczeństwem IT. Jednak, jak pokazują ataki ransomware "Prestige" na kluczową infrastrukturę logistyczną w Polsce, wsparcie ukraińskiej infrastruktury z państw trzecich również może być zagrożone.

Podsumowanie

Niektórzy zachodni eksperci ds. cyberbezpieczeństwa spodziewali się, że Rosja przeprowadzi masowe operacje cybernetyczne w połączeniu z konwencjonalnymi działaniami wojennymi na Ukrainie, co prawdopodobnie nie miało miejsca. Zamiast tego rosyjscy cyberprzestępcy brali udział w operacjach cybernetycznych, koncentrując się na dezinformacji i szpiegostwie, celem wsparcia konwencjonalnych działań wojennych i sił okupacyjnych. W miarę jak fluktuowały rosyjskie cyberoperacje, Ukraina, z wydatną pomocą swoich przyjaciół, podjęła walkę w cyberprzestrzeni, udaremniając wiele rosyjskich operacji ofensywnych i wykorzystując słabą obronę cybernetyczną Rosji.

Pomoc cybernetyczna udzielana przez różne podmioty w samoobronie Ukrainy ustanowiła (wstępną) praktykę państwową polegającą na niedeklarowanym powstrzymywaniu się od działań wojennych, co skutkuje różnymi formami współpracy operacyjnej poniżej normatywnego progu bezpośredniego udziału w działaniach wojennych. Prawdopodobnie pomoc ta nie przyczyniła się do eskalacji konfliktu, ponieważ bezprawna agresja na Ukrainę została udaremniona, a agresor milczał na temat (nie)legalności wsparcia cybernetycznego. Nie dajmy się jednak zwieść pozorom jeśli chodzi o możliwość uogólnienia tego stwierdzenia: po pierwsze, niewielu agresorów rozpocznie działania wojenne bez odpowiedniego przygotowania, wyciągając wnioski i rosyjskich doświadczeń na Ukrainie i niewielu będzie miało zasoby po temu, aby skuteczniej wykorzystać ofensywne zdolności cybernetyczne, które Rosja wykorzystała w pierwszym miesiącu działań wojennych. Po drugie, podczas gdy demokratyczne państwa pospieszyły z cybernetyczną pomocą Ukrainie w sposóbnieskoordynowany, jest mało prawdopodobne, aby ponownie tak działały. W miarę jak operacyjna współpraca cybernetyczna staje się coraz bardziej powszechna i skuteczna, Rosja i inne podmioty będą bardziej skłonne do rozwiązywania problemów przy pomocy metod prawnych, politycznych lub wojskowych. Aby zagwarantować, iż skutki wzmocnionej współpracy operacyjnej nie doprowadzą do eskalacji konfliktu, państwa demokratyczne powinny zachować przejrzystość w zakresie koncepcji i praktyk prawnych, tak aby normy dotyczące powstrzymywania się od udziału w konflikcie zbrojnym w cyberprzestrzeni, oscylując poniżej progu użycia siły, mogły dalej się rozwijać.

Pomoc informatyczna udzielana Ukrainie przez różne podmioty niepaństwowe była wydajna i prawdopodobnie skuteczna przy próbach obnażenia słabości rosyjskich cyberataków i jej cybernetycznej obrony. Na razie władze rosyjskie zdają się traktować je jedynie jako swoistą uciążliwość, uznając za ważniejsze działanie najemników konwencjonalnych, jak np. Grupa Wagnera. Jednak w miarę jak działania wojenne przechodzą do następnego etapu, a braki kadrowe i amunicji stają się oczywiste, dyscyplina operacyjna ze strony podmiotów niepaństwowych, zwłaszcza armii informatycznej, powinna być poddana skrupulatnej analizie. W miarę rozwoju konwencjonalnych działań wojennych w 2023 r. staranność przy zabezpieczaniu sieci informatycznych może wymagać większych nakładów, a tym samym stać się elementem walki, z którym Rosja musi się liczyć. Ponieważ Rosja wykorzystuje morderstwa polityczne poza swoimi granicami do różnych celów, można sobie wyobrazić, że operacje cybernetyczne mogą wywierać skutki ponownie w sferze walki konwencjonalnej.

Ponadto, jak zauważyła Erica Lonergan, zwerbowanie przez Ukrainę międzynarodowej ochotniczej cyberarmii może pozostawać w sprzeczności z wysiłkami innych państw, zmierzających do wykształcenia modelu odpowiedzialnego zachowania w cyberprzestrzeni, zwłaszcza w kontekście międzynarodowych cyberataków. Jeśli niektóre niezależne grupy atakują cywilną infrastrukturę krytyczną w Rosji, oświadczając publicznie, że odpowiadają proporcjonalnie na rosyjskie ataki na Ukrainie, można sobie wyobrazić, że Rosja może pociągnąć do odpowiedzialności rządy pozwalającej owym grupom na działanie ze swoich terytoriów.

Co więcej, o ile niektóre państwa interpretują normy prawa międzynarodowego jako zakazujące ataków na infrastrukturę krytyczną, w odróżnieniu od operacji mających na celu jedynie uzyskanie dostępu do danych, w tym danych wywiadowczych, długotrwała zależność Ukrainy od "jednostek nieregularnych" umożliwia kwalifikację państw wspierających grupy udzielające je pomocy jako takich, które nie zawahają się przed poszerzeniem katalogu atakowanych celów, bez względu na konsekwencje w stosunkach międzypaństwowych. Dlatego też państwa wspierające Ukrainę powinny ustalić bardziej rygorystyczne zasady, w oparciu o które będą wyrażać swoją solidarność w cyberprzestrzeni, zwłaszcza wobec intensyfikacji działań wojennych.

Po trzecie, firmy informatyczne odegrały kluczową rolę w obronie Ukrainy udzielając "schronienia" w cyberprzestrzeni i wsparcia operacyjnego jej naczelnym organom i przechowując dane, z których korzystają. W ten sposób zdobyły informacje o instrumentach państwowej obrony cybernetycznej, a tym samym, w ocenie niektórych rządów, bardzo silną pozycję w przypadku potencjalnej współpracy. Takie

ścisłe partnerstwo publiczno-prywatne w zakresie cyberobrony operacyjnej czasowo może być konieczne. Jednak w miarę jak staje się ona ponadnarodowa, jej prawne i polityczne implikacje muszą być poddane szczegółowej analizie i uregulowane. Jak pokazuje kluczowe wsparcie firmy Starlink dla wojny konwencjonalnej na Ukrainie, zachowanie prywatnych podmiotów gospodarczych może wywoływać bezpośrednie konsekwencje w obszarze stosunków międzypaństwowych. Oznacza to, że ich zachowanie musi stanowić kryterium przy ustalaniu progu ataku zbrojnego i działań wojennych w cyberprzestrzeni, także tych realizowanych przez podmioty prywatne działającej pod kontrolą i na zlecenie władz państwowych.

Zalecenia polityczne

- W niniejszym opracowaniu wykazaliśmy, że operacje cybernetyczne wspierające prawo Ukrainy do indywidualnej samoobrony zgodnie z art. 51 są legalne, jeśli nie są realizowane w ramach bezpośredniej kontroli operacyjnej, są proporcjonalne i nie obejmują działań niezgodnych z prawem.

- Działania wspierające w cyberprzestrzeni w ramach realizacji prawa do indywidualnej samoobrony na podstawie art. 51 nie pojawiają się często, bowiem i nieczęste są konflikty międzypaństwowe w cyberprzestrzeni. Jednak w miarę jak coraz więcej państw włącza operacje cybernetyczne do katalogu instrumentów realizacji polityki bezpieczeństwa i prawa do obrony, praktyka państwowa wyraźnie ewoluuje.

- Ponieważ operacje cybernetyczne prowadzone przez podmioty niepaństwowe i cybernajemników występowały powszechne w wojnie rosyjsko-ukraińskiej, podkreślamy, że zasada należytej staranności musi być interpretowana jako nakazując powściągliwość podmiotów prywatnych celem przeciwdziałania potencjalnej eskalacji skutków " obywatelskiej cyberobrony".

- Cyberobrona obywatelska stwarza znaczne ryzyko zatarcia granic między dopuszczalnymi działaniami obronnymi a bezpośrednimi szkodami operacyjnymi, ponieważ podmioty niepaństwowe mogą nietrafnie zakładać, że nie ich działania nie dadzą podstaw do odpowiedzialności międzynarodowej państwa, z terytorium którego lub pod kontrola którego operują.

- Wsparcie ofensywnych działań cybernetycznych z pewnością doprowadzi do ponownego wyznaczenia cienkiej linii "bezpośrednich szkód operacyjnych", a tym samym będzie miało poważne konsekwencje dla ustalenia statusu stron walczących i granic zbiorowej samoobrony.

- W celu dalszego rozwoju i implementacji zasad prawa międzynarodowego, a w szczególności Karty Narodów Zjednoczonych, państwa wspierające Ukrainę powinny zgłaszać Radzie Bezpieczeństwa ONZ swój status, określając w bardziej przejrzysty sposób progi prawne pozwalające nadać im status państwa nieuczestniczącego w konflikcie.

- Aby uniknąć eskalacji konfliktów w cyberprzestrzeni, państwa wspierające Ukrainę powinny w zaufaniu dzielić się interpretacjami norm prawnych, które leżą u podstaw realizacji przez nie pomocy dla zaatakowanej strony, z członkami Rady Bezpieczeństwa ONZ, w tym z Rosją.

- Aby złagodzić ryzyko eskalacji konfliktu, wynikające z działań podmiotów niepaństwowych, zarówno najemników cybernetycznych, jak i konwencjonalnych, państwa świadomie goszczące członków Armii IT Ukrainy powinny współpracować z ukraińskim rządem. Celem tego zaangażowania powinno być podkreślenie przez władze ukraińskie w ewentualnych przyszłych rozmowach z władzami rosyjskimi konieczności budowania zaufania między stronami w działaniach wojennych poprzez ograniczanie działań podmiotów niepaństwowych, tj. zarówno konwencjonalnych, jak i cybernetycznych.

- Państwa grupy G-7 powinny bliżej przyjrzeć się roli, jako w tym konflikcie i jego ewentualnej eskalacji odgrywają platformy społecznościowe oraz firm pomagające rządom państw w cyberobronie. W tym celu powołana mogłaby zostać grupa robocza. Celem takiej grupy roboczej powinno być opracowanie katalogu zasad i procedur regulujących ponadnarodową pomoc cybernetyczną udzielaną przez podmioty prywatne. Jej celem nadrzędnym powinna być ochrona integralności i suwerenności państw przez cały czas trwania konfliktu, przy jednoczesnym umożliwieniu tymczasowej pomocy ze strony kompetentnych firm informatycznych, tak aby zapewnić implementację istniejących norm prawnych i reguł odpowiedzialność państwa, tj. w szczególności zasadę należytej staranności.

O autorach:

- **Martin Müller** jest asystentem uniwersyteckim i doktorantem w Instytucie Teorii i Przyszłości Prawa na Uniwersytecie w Innsbrucku.
- **Prof. Dr. Sebastian Harnisch** jest profesorem stosunków międzynarodowych i polityki zagranicznej na Uniwersytecie w Heidelbergu.
- **Tłumaczenie polskie: Dr Joanna Kulesza** jest adiunktem w Katedrze Prawa Międzynarodowego i Stosunków Międzynarodowych Wydziału Prawa i Administracji Uniwersytetu Łódzkiego oraz kierownikiem centrum badawczego Lodz Cyber Hub.