Szanowni Państwo,

oddajemy w Państwa ręce pierwszy numer nowego czasopisma. Zadaniem „Cybersecurity & Law" ma być inspirowanie do pogłębionych analiz, wymiany poglądów, stawiania pytań i poszukiwania odpowiedzi. Zakres możliwych do poruszenia tematów jest niezwykle szeroki. Postęp technologiczny sprawia, że coraz większa ilość procesów staje się wręcz niemożliwa do przeprowadzenia bez cyfrowego wsparcia. Rośnie znaczenie i dostępność Internetu Rzeczy (iOT – Internet of Things), już przeszło 10 lat temu urządzeń stale podłączonych do globalnej sieci było więcej niż ludzi, a wkrótce ich liczba może sięgnąć 50 miliardów. Stale rozwijają się mechanizmy uczenia maszynowego (machine learning) i sztucznej inteligencji (AI – artificial intelligence), a rdzeniem organizującym cyfrową rzeczywistość stanie się już niedługo sieć 5G, której komercyjne wdrożenia dopiero się rozpoczęły, podczas gdy kilka krajów, w tym oficjalnie Chiny, pracuje już nad standardem 6G. Cyfrowa rzeczywistość stała się w sposób naturalny wyzwaniem dla osób i instytucji odpowiadających za bezpieczeństwo w wymiarze krajowym i międzynarodowym. Cyberprzestrzeń to bowiem oczywiście nie tylko nowe usługi, ułatwienia, czy kanały komunikacji i rozrywka. To jednocześnie atrakcyjne środowisko do działania dla grup przestępczych i terrorystycznych, a także państw, które przy jej wykorzystaniu mogą realizować rozbudowane operacje wywiadowcze, polityczne, czy socjotechniczne oraz dokonywać swoistej projekcji siły. Działania w cyberprzestrzeni mogą być także przygotowaniem do podjęcia lub elementem trwających operacji militarnych.

Nie zaskakuje zatem, iż zgodnie z decyzjami NATO cyberprzestrzeń została uznana za domenę operacyjną działań militarnych. W deklaracji końcowej szczytu NATO, który odbył się w Walii w 2014 r. Sojusz potwierdził, iż należy mieć świadomość, że „zagrożenia i ataki cybernetyczne będą coraz częstsze, bardziej złożone i potencjalnie niszczące". Jednocześnie potwierdzono wówczas, że „obrona cybernetyczna należy do podstawowych zadań kolektywnej

obrony NATO", zwracając jednocześnie uwagę na możliwość zastosowania w przypadku ataku w cyberprzestrzeni art. 5 Traktatu Północnoatlantyckiego. Podczas szczytu warszawskiego w 2016 r. NATO potwierdziło swój mandat do obrony w tej sferze i uznało cyberprzestrzeń za obszar działań, w którym musi bronić się tak samo skutecznie jak w powietrzu, na lądzie i na morzu. Podczas szczytu NATO w Brukseli w 2018 r. podkreślono znaczenie tworzenia nowej domeny działań operacyjnych sojuszu. Zapadła też decyzja o reformie struktur dowodzenia NATO i utworzeniu Centrum Operacji Cyberprzestrzeni (ang. Cyberspace Operations Center) w Mons w Belgii wchodzącego w skład struktury dowodzenia NATO.

Podkreślenia wymaga, że cyberprzestrzeń to jedyna domena operacyjna wymyślona, stworzona i prawie dowolnie modyfikowana przez człowieka wedle jego kreatywności i potrzeb. To człowiek najlepiej zna prawa nią rządzące i potrafi wykorzystywać do swoich celów jej zalety. Operacje w cyberprzestrzeni charakteryzują się kilkoma wspólnymi cechami, które wpływają na atrakcyjność wykorzystania tej domeny. Przeprowadzenie ataku w cyberprzestrzeni jest stosunkowo tanie, szybkie, nie wymaga zaangażowania dużego zespołu, a często nie wymaga nawet samodzielnego dysponowania pogłębioną wiedzą, gdyż zlecenie odpowiednio zdefiniowanej „usługi", czy nabycie i wykorzystanie służących do wrogiego działania narzędzi nie nastręcza wielu trudności. Oczywiście istotny jest globalny charakter sieci, dzięki czemu możliwość operowania na terenie innego kraju nie wymaga fizycznej obecności na jego terytorium. W tym zakresie zmiany może przynieść wdrożenie koncepcji swoistego internetowego izolacjonizmu, czyli możliwość odcięcia się od transgranicznych węzłów komunikacyjnych, nad czym aktywnie pracuje wiele krajów, w tym Rosja, która przyjęła nawet stosowną ustawę. Cyberprzestrzeń to także cały czas stosunkowa łatwość ukrycia tożsamości, co znacząco utrudnia atrybucję, warunkującą następnie możliwość zastosowania precyzyjnej i adekwatnej odpowiedzi. Nieograniczona inwencja atakujących sprawia, że każdego dnia powstają nowe metody i narzędzia. Cechy cyberprzestrzeni jako domeny operacyjnej działają więc na korzyść tych wszystkich, którzy przy jej pomocy chcą prowadzić wrogie działania. Tym trudniejsza jest rola osób i struktur odpowiedzialnych za zapewnienie cyberbezpieczeństwa.

Także z tych powodów geostratedzy zwracają uwagę, iż charakter cyberprzestrzeni i zdolność do jej wykorzystania jako domeny operacyjnej skraca znacząco dystans między krajami na różnym poziomie rozwoju. Pozwala też na dążenie do dołączenia do grona regionalnych lub nawet globalnych potęg

krajom, które pod względem potencjału militarnego i gospodarczego nigdy nie mogłyby na to liczyć.

W Polsce kwestie dotyczące cyberbezpieczeństwa traktujemy niezwykle poważnie. To wyzwanie związane przede wszystkim z otoczeniem bezpieczeństwa kraju wschodniej flanki NATO. Bogate tradycje polskiej kryptologii, czy lwowskiej szkoły matematycznej, ale też teraźniejszość, w której możemy być dumni z międzynarodowych osiągnięć polskich uczniów, studentów, specjalistów i ekspertów w zakresie matematyki, czy informatyki, predestynują nasz kraj do odgrywania w cyfrowym świecie istotnej roli.

Na poziomie strategicznym polski rząd dokonał stosownych rozstrzygnięć. W sierpniu 2018 r. weszła w życie pierwsza polska ustawa o krajowym systemie cyberbezpieczeństwa, która stanowi, iż krajowy system opiera się co do zasady na trzech filarach: MON, ABW i NASK-PIB, odpowiedzialnych za prowadzenie działających na poziomie krajowym Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT MON, CSIRT GOV i CSIRT NASK). Ustawa określiła też zadania ministra obrony narodowej, do których należy m.in.:

– zapewnienie zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych – w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych;

– rozwijanie umiejętności Sił Zbrojnych Rzeczypospolitej Polskiej w zakresie zapewnienia cyberbezpieczeństwa przez organizację specjalistycznych przedsięwzięć szkoleniowych;

– pozyskiwanie i rozwój narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych Rzeczypospolitej Polskiej oraz

– prowadzenie Narodowego Punktu Kontaktowego do współpracy z NATO, którego celem ma być m.in. dział w realizacji celów Organizacji Traktatu Północnoatlantyckiego w obszarze cyberbezpieczeństwa i kryptologii.

Jednocześnie, stosownie do postanowień Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017–2022, przyjętych uchwałą Rady Ministrów z dnia 27 kwietnia 2017 r. ustalono cztery cele szczegółowe:

1) osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa;

2) wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom;

3) zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni;

4) zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa.

Natomiast, w zastępującej Krajowe Ramy Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, przyjętej uchwałą Rady Ministrów z dnia 22 października 2019 r. określono pięć celów szczegółowych:

1) rozwój krajowego systemu cyberbezpieczeństwa;

2) podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty;

3) zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa;

4) budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa;

5) zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

W wyniku prac zainicjowanych w MON, w marcu 2018 r. pod moim kierunkiem, powstał kompleksowy program podniesienia zdolności do działania w cyberprzestrzeni pod nazwą CYBER.MIL.PL, którego założenia przedstawiono publicznie w lutym 2019 r. Działania i zamierzenia MON ujęto w kilkudziesięciu projektach, które można tematycznie podzielić na cztery grupy:

1. Konsolidacja i budowanie struktur odpowiedzialnych za cyberbezpieczeństwo oraz zwiększenie zdolności do działania w cyberprzestrzeni.

2. Edukacja, szkolenie, trening.

3. Współpraca międzynarodowa i budowanie silnej pozycji międzynarodowej.

4. Podniesienie poziomu bezpieczeństwa resortowych i wojskowych sieci i systemów.

Jednym z projektów zidentyfikowanych w ramach drugiego filaru było także uruchomienie czasopisma naukowego poświęconego zagadnieniom cyberbezpieczeństwa. Także i ten projekt możemy wraz z wydaniem pierwszego numeru uznać za zrealizowany.

Dlaczego „Cybersecurity & Law"? Bo ważne, aby do przeszłości odeszło niesłuszne, a niestety ugruntowane przekonanie, że cyberbezpieczeństwo to domena informatyków i działów IT. Nie, zapewnienie cyberbezpieczeństwa to wyzwanie przekrojowe, które w różnym stopniu dotyka każdego z nas. To ogromny obszar, w którym rośnie zapotrzebowanie na różnego rodzaju

kompetencje, często zupełnie niezwiązane ze stricte technicznymi umiejętnościami. Analiza prawna, zarówno w zakresie prawa administracyjnego, karnego, cywilnego, jak europejskiego czy międzynarodowego, a także refleksja systemowa i organizacyjna stale towarzyszą pracom prowadzonym w ramach nowej domeny operacyjnej.

Redaktor naczelnej i całemu zespołowi czasopisma gratuluję pierwszego numeru i życzę wytrwałości, pasji i kreatywności w dążeniu do stałego doskonalenia tego niezwykle ciekawie zapowiadającego się nowego tytułu!

Tomasz Zdzikot
sekretarz stanu w MON
pełnomocnik ministra obrony narodowej
do spraw bezpieczeństwa cyberprzestrzeni