Wstęp

> Zjawisko Internetu przypomina poniekąd znany nam z Biblii potop, czyli nadmiar wód w którym można ze wszystkim utonąć, jeżeli nie zdołamy dla ratunku, jak Noe, zbudować sobie Arki.
>
> Ale jakby miała wyglądać „Arka Noego Internetu..." ?
>
> *S. Lem*, Bomba megabitowa, Kraków 1999, s. 13

Informatyzacji i rozwojowi elektronicznych usług towarzyszą nowe zagrożenia związane z naruszeniem poufności, integralności i dostępności informacji oraz wzrostem niepewności co do jej pochodzenia. Zakłócenia funkcjonowania sieci i systemów informacyjnych mogą oddziaływać zarówno na jednostki jak i zbiorowości, podmioty prywatne i publiczne, poszczególne państwa i organizacje międzynarodowe. Mogą mieć wymiar lokalny, krajowy i międzynarodowy ze względu na ścisłe powiązanie zagrożeń bezpieczeństwa państwa i obywateli z problemami geopolitycznymi oraz globalizacją.

Coraz większym zagrożeniem stają się celowe działania podejmowane przez cyberprzestępców w ramach zorganizowanych grup, organizacji o charakterze terrorystycznym a także wywiadów obcych państw. Do szybkiego wzrostu ilości cyberprzestępstw przyczynia się możliwość osiągnięcia przez sprawców znacznych korzyści przy stosunkowo niskim ryzyku wykrycia – w szczególności dzięki wykorzystaniu narzędzi anonimizujących czy posłużeniu się uprzednio skradzioną tożsamością.

Nowa generacja cyberprzestępstw to zautomatyzowane, rozproszone ataki przeprowadzane z wykorzystaniem napisanego w tym celu oprogramowania. Cyberprzestępczość ma również transgraniczny charakter, co utrudnia ściganie sprawców i zabezpieczanie dowodów, a także wymusza międzynarodową współpracę i koordynację podejmowanych działań. Rosnący zakres działań cyberprzestępców pokazują skuteczne ataki na globalne spółki, systemy bankowe czy dokonane pod koniec 2016

roku włamania do instytucji finansowych i podmiotów publicznych na całym świecie, w tym również w Polsce.

Ataki mogą być ukierunkowane nie tylko na osiągnięcie zysku przez sprawców, ale również na pozyskanie informacji, wpływanie na decyzje o charakterze strategicznym lub nastroje społeczne oraz powodowanie destabilizacji zarówno politycznej jak i gospodarczej. Jako jedno z zagrożeń dla podstaw społeczeństwa informacyjnego wskazuje się post-prawdę, zaś zjawisko *fake-news* zostało dostrzeżone jako instrument politycznego wpływu w mediach społecznościowych oddziałujący na decyzje podejmowane przez wyborców. Kampanie dezinformacyjne oraz ataki na infrastrukturę informacyjną są również istotnym elementem wojny hybrydowej cechującej się łączeniem różnych środków i metod przemocy, w tym zwłaszcza zbrojnych działań regularnych i nieregularnych, operacji w cyberprzestrzeni oraz działań ekonomicznych, psychologicznych czy kampanii informacyjnych. Potwierdza to pogląd Stanisława Lema, że polityka to „dziedzina, w której Internet może się przyczynić do zła o wiele szybciej, łatwiej, pewniej, aniżeli do dobra", albowiem jest takim rodzajem łączności, który łatwiej pozwala ustalić adresatów informacji niż nadawców informację ślących, a w sferze polityki ta różnica może nawet „stanowić różnicę między pokojem a wojną"[1].

Pojawienie się nowych modeli przetwarzania danych i związanych z nimi zagrożeń spowodowało rozchwianie istniejącego modelu ochrony bezpieczeństwa państw, instytucji, przedsiębiorców oraz obywateli. Związane z informatyzacją zmiany w stosunkach społecznych i gospodarczych implikują konieczność podjęcia działań mających na celu zapewnienie bezpieczeństwa w cyberprzestrzeni. Działania te obejmują określenie celów strategicznych i środków dla ich realizacji - w tym zwłaszcza działań legislacyjnych i normalizacyjnych, zdefiniowania zadań publicznych związanych z zapewnieniem ładu w cyberprzestrzeni a także określenia podmiotów odpowiedzialnych za cyberbezpieczeństwo i ich kompetencji.

Inicjatywy związane z zapewnieniem cyberbezpieczeństwa i przeciwdziałaniem cyberprzestępczości podejmowane są przez organizacje międzynarodowe, poszczególne kraje czy globalne korporacje. Działania Unii Europejskiej wynikają z celów określonych w Europejskiej Agendzie Cyfrowej oraz przyjętej w lutym 2013 r. „Strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń". Dla realizacji celów w niej określonych podjęto prace legislacyjne, których rezultatem jest m.in. dyrektywa 2016/1148 z 6.7.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. W działania wspierające budowę bezpieczeństwa cyberprzestrzeni wpisują sie także inne inicjatywy – w tym rozporządzenie Parlamentu Europejskiego i Rady (UE) 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE oraz rozporządzenie 2016/679

[1] *S. Lem*, Bomba megabitowa, Kraków 1999 s. 13–14.

w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Na forum Rady Europy i Unii Europejskiej podejmowane są również działania mające na celu stanowienie norm wyznaczających ramy współpracy międzynarodowej państw zaangażowanych w zwalczanie cyberprzestępczości do których zaliczyć można Konwencję Rady Europy z 23.11.2001 r. o cyberprzestępczości oraz Dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE z 12.8.2013 r. dotyczącą ataków na systemy informatyczne.

W Polsce zakończono prace nad Strategią Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Trwają prace nad ustawą o krajowym systemie cyberbezpieczeństwa, implementującą do porządku krajowego dyrektywę NIS. Na zwalczanie cyberzagrożeń powinna wpłynąć również realizacja wysuwanych przez współautorów tej monografii postulatów. Odnoszą się one w szczególności do koordynacji infrastruktury informacyjnej państwa, wspierania ośrodków i rozproszonych zespołów eksperckich, stworzenia ram certyfikacji bezpieczeństwa ICT, wspierania partnerstwa prywatno-publicznego na rzecz inwestycji w zakresie cyberbezpieczeństwa, dostosowania ustawodawstwa karnego do postanowień Konwencji Rady Europy z 23.11.2001 r. o cyberprzestępczości oraz Dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE.

Pilnie potrzebne jest także szeroko zakrojone uczenie „żeglowania" po coraz bardziej wzburzonym „oceanie danych" – w tym zwłaszcza dostosowanie kompetencji zatrudnionych w sektorze publicznym do aktualnych potrzeb w zakresie ochrony przed cyberzagrożeniami.

Agnieszka Gryszczyńska i Grażyna Szpor