Cyberbezpieczeństwo gwarantem cyfrowej globalizacji

Dominika Bettman
Dyrektor Generalna, Microsoft Polska

Coraz częściej słychać głosy o nasilającej się deglobalizacji. Czy dotknie ona również świata cyfrowego? Tutaj wydaje się, że mamy do czynienia z trendem wręcz odwrotnym – technologie w coraz większym stopniu łączą ludzi. Niesie to zarówno ogrom nowych szans, jak i mnogość zagrożeń. Kluczem do wykorzystania tych pierwszych i zażegnania drugich, jest cyberbezpieczeństwo. By je zapewnić potrzebna jest gra zespołowa.

Wojna w Ukrainie — drugi potężny kryzys, jaki nastąpił zaraz po szoku wywołanym pandemią COVID-19, spotęgował światową recesję i sprowokował dyskusję o nieuchronności deglobalizacji. Poszczególne państwa, ale i całe kontynenty rozpoczęły działania mające prowadzić do większej samowystarczalności w kontekście handlowym.

Skracanie i dywersyfikowanie łańcuchów dostaw faktycznie nosi znamiona deglobalizacji. Jednocześnie, za sprawą usieciowienia wielu aspektów życia, (mega)globalizacja, choć przetasowana, wciąż jest faktem. Nazwijmy ją „globalizacją informacyjną". Powiązania rynków i konsumentów, wspierane przez nowe technologie, ułatwiona i przyspieszona wymiana wiedzy, a także swobodne interakcje między ludźmi i instytucjami — niezależnie od lokalizacji — otwierają tyle samo szans, co wyzwań. „Globalna wioska" (jak nazwał połączony za sprawą Internetu świat Marshall McLuhan) stawia dziś czoła nowym formom ryzyka: nie tylko fizycznego, ale coraz częściej i cybernetycznego.

Skracanie i dywersyfikowanie łańcuchów dostaw faktycznie nosi znamiona deglobalizacji. Jednocześnie, za sprawą usieciowienia wielu aspektów życia, (mega) globalizacja, choć przetasowana, wciąż jest faktem.

Epoka społeczeństwa informacyjnego

Już od ponad dwóch dekad eksperci OBWE i NATO mówią o globalnym, „kooperatywnym" bezpieczeństwie. Obejmuje ono: ochronę przed monopolizacją rynków i protekcjonizmem, poszanowanie szybko kurczących się zasobów surowcowych i źródeł energii, stabilność finansową, dbałość o środowisko oraz równowagę i dobrobyt społeczeństwa. Społeczeństwa informacyjnego, które w każdym swoim aspekcie bazuje na danych: ich przetwarzaniu i dystrybucji.

Za sprawą nowych środków komunikacji, zwłaszcza elektronicznych, szybkość przekazywania informacji, ich ilość i dostępność jest niewspółmiernie wyższa niż kiedykolwiek wcześniej w historii ludzkości. Technologie informacyjne są odmiejscowione.

Do klasycznych podziałów społecznych (tj. tworzonych na podstawie przynależności narodowej, kulturowej czy wyznaniowej etc.) dochodzą dziś „podziały ponad granicami" — np. kooperacyjne, w obszarach, takich jak nauka, polityka, sztuka, technika, turystyka czy współdzielone hobby. Transformacja cyfrowa obejmuje także sektory krytyczne — przemysł, transport, energetykę, zdrowie i finanse. Całe gospodarki stają się coraz bardziej zdigitalizowane i wyrafinowane technologicznie.

Należy przy tym pamiętać, że digitalizacja to miecz obosieczny: transformacja cyfrowa jest w stanie optymalizować (ułatwiać i przyspieszać) podejmowanie wielu codziennych decyzji — tak w kwestiach społecznych, jak i biznesowych czy politycznych. Jednocześnie ilość wiadomości, z jaką jesteśmy na co dzień konfrontowani, może wymykać się spod kontroli. Ludzka bezradność wobec zalewu informacji otwiera furtkę do nadużyć, z której na różne sposoby korzystają cyberprzestępcy. Zagrożenia w tej przestrzeni mają wiele twarzy. Oprócz ataków na systemy IT (rozumiane w ściśle techniczny sposób), obserwujemy dynamiczną tendencję wzrostową ataków ukierunkowanych, motywowanych politycznie, społecznie czy ekonomicznie. Coraz większe znaczenie zyskują też tzw. *fake news* oraz inne zjawiska służące polaryzacji społecznej.

> **Digitalizacja to miecz obosieczny: transformacja cyfrowa jest w stanie ułatwiać podejmowanie wielu codziennych decyzji. Jednocześnie ilość wiadomości, z jaką jesteśmy na co dzień konfrontowani, może wymykać się spod kontroli.**

W obliczu cyberzagrożenia

W 2021 roku, podczas World Economic Forum w Davos, zagrożenia cybernetyczne zakwalifikowano na czwartym miejscu pod względem częstotliwości występowania, czyli za chorobami zakaźnymi, kryzysem gospodarczym i ekstremalnymi zjawiskami pogodowymi. Cyberprzestępstwa, które w tym niechlubnym rankingu wyprzedzają fizyczne ataki terrorystyczne, generują zyski przewyższające przychody z produkcji i sprzedaży narkotyków (przy ciągłej tendencji wzrostowej!). W ostatnich latach hakerzy przekształcili się z działających w pojedynkę przestępców, w systemowo połączone i wspierane przez wpływowe środowiska — często polityczne — grupy cyberterrorystyczne („haktywistów"). Ich ofiarami padają rządy, instytucje i korporacje; bronią jest naruszanie i wykorzystywanie danych, szpiegostwo czy kradzież tożsamości; a celem — generowanie strat finansowych na wielką skalę, zakłócenia funkcjonowania społeczeństw, podważanie reputacji organizacji.

Przykład wojny w Ukrainie pokazał wyraźnie, że do tej wyliczanki bezwzględnie należy dodać zagrożenie bezpieczeństwa fizycznego. Sponsorowane przez państwa totalitarne narzędzia technologiczne są wykorzystywane do ataków w przestrzeni cybernetycznej, przejmowania danych wywiadowczych, inwigilacji sił zbrojnych i niszczenia infrastruktury krytycznej. W efekcie oznacza to krzywdę, a nierzadko i śmierć niewinnych ludzi.

> **W ostatnich latach hakerzy przekształcili się z działających w pojedynkę przestępców, w systemowo połączone i wspierane przez wpływowe środowiska grupy cyberterrorystyczne („haktywistów").**

Musimy sobie uświadomić, że zagrożenia cybernetyczne mają potencjał do wszczęcia, w określonych okolicznościach, procedury z mocy art. 5 Traktatu Północnoatlantyckiego (czyli tzw. zasady „jeden za wszystkich, wszyscy za jednego"). Zgodnie z nią cały sojusz NATO zobowiązany jest do mobilizacji w razie ataku na jedno

z państw członkowskich. Nie bez przyczyny cyberprzestrzeń została uznana przez NATO za pełnoprawną domenę działań wojennych, obok lądu, morza, powietrza i przestrzeni kosmicznej. Obejmuje ona nie tylko sieci informacyjno-telekomunikacyjne, infrastrukturę i dane krytyczne, ale także umożliwia działanie kluczowych systemów mających wpływ na utrzymanie ciągłości funkcjonowania państwa i jego obywateli.

Tego, jak strategiczną rolę w zachowaniu ciągłości administracji publicznej odgrywa technologia, dowiodły działania wojenne w Ukrainie. Dostrzegając wrażliwość rządowej infrastruktury serwerowej w sferze fizycznej oraz cybernetycznej, tydzień przed inwazją Rosji, ukraiński parlament zdążył przegłosować poprawkę, pozwalającą na migrację danych do chmury publicznej. W ciągu 10 tygodni przeniesiono krytyczne dane oraz procesy ponad 20 ministerstw, oraz 100 agencji i firm państwowych. Uchroniło je to przed zniszczeniem, gdyż na liście pierwszych celów rosyjskich ataków rakietowych oraz cybernetycznych były właśnie rządowe centra danych Ukrainy.

Jak się chronić?

Rozwiązania takie jak chmura są przykładem już nie mega-, a hiperglobalizacji naszych czasów. Chmura funkcjonuje ponad granicami. Łączy podmioty z całego globu, dając im tym samym zmasowaną siłę sprawczą przeciwko zorganizowanej cyberprzestępczości. Bo bezpieczeństwo cybernetyczne to gra zespołowa. Wobec skali współczesnych zagrożeń nikt — żadna firma ani żaden rząd, nie jest w stanie obronić się w pojedynkę.

Technologie to jedno; kolejnym niezbędnym aspektem zapewniającym globalne cyberbezpieczeństwo, jest wspierające ustawodawstwo oraz partnerstwo międzynarodowe i transkontynentalne. Rządy i instytucje muszą tworzyć strategie odpornościowe i realizować je w jeszcze bardziej skoordynowany sposób, angażując we współpracę różnych interesariuszy. Budowanie systemowej odporności wymaga zaangażowania całego społeczeństwa, administracji i gospodarki oraz stworzenia ram współpracy we wszystkich możliwych wymiarach bezpieczeństwa. Szczególnie w tych, które zostały zdefiniowane przez NATO. Wzmacnianie przez państwa członkowskie odporności w tych obszarach jest wypełnieniem zobowiązania zapisanego w artykule 3. Traktatu Północnoatlantyckiego (rozwijanie indywidualnej zdolności do odparcia napaści) i jest warunkiem skutecznej obrony kolektywnej opisanej w art. 5.

> **Bezpieczeństwo cybernetyczne to gra zespołowa. Wobec skali współczesnych zagrożeń nikt – żadna firma ani żaden rząd, nie jest w stanie obronić się w pojedynkę.**

Powyższe przykłady pokazują, że deglobalizacja nie obejmuje przestrzeni cybernetycznej. Bez względu na dzielące ludzi na całym świecie różnice (poglądów, kultur czy wyznań), łączy ich technologia i konieczność ochrony przed zagrożeniami „w sieci". Globalizacja (cyfrowa) ma się dobrze, ale gwarantem jej funkcjonowania jest cyberbezpieczeństwo.

O autorce

Dominika Bettman – przedsiębiorczyni, orędowniczka nowych technologii i zrównoważonego biznesu. Od grudnia 2021 Dyrektor Generalna Microsoft w Polsce, odpowiedzialna za wdrożenie projektu Polskiej Doliny Cyfrowej.

Wcześniej CEO Siemens Sp. z o.o. Absolwentka Wydziału Handlu Zagranicznego SGH w Warszawie i Advanced Management Program IESE w Barcelonie.

Propagatorka idei różnorodności i przywództwa włączającego. Autorka książki „Technologiczne magnolie".