DOI 10.24917/9788380841390.8

RADOSŁAW MARZĘCKI

Instytut Politologii
Uniwersytet Pedagogiczny im. KEN w Krakowie

Poczucie zagrożenia cyberprzestępczością. Zróżnicowanie międzynarodowe

Wprowadzenie

Dynamika zmian, jakim podlega współczesny świat, znacząco utrudnia jego szczegółowy opis i niemal uniemożliwia precyzyjne prognozowanie przyszłości. Charakterystyka tych transformacji w dużej mierze determinowana jest rozwojem i rozprzestrzenianiem się nowych technologii, które modyfikują podstawy funkcjonowania społeczeństw we wszelkich możliwych aspektach: politycznym, gospodarczym czy kulturowym[1]. Dziś trudno sobie wyobrazić codzienne życie bez narzędzi, które przyczyniły się do tych zmian[2]. Komputer jako narzędzie oraz internet jako przestrzeń działania stanowią, jak twierdzą autorzy pracy *Świat digital natives*,

> jedno z największych wyzwań naszych czasów. Dostęp do niej, zmieniając pojęcia: wolności, prawdy, inteligencji, interakcji i więzi społecznych, powoduje, że informatyczność, kreując nową rzeczywistość społeczną, może albo prowadzić w stronę pozytywnych zmian i zapewnienia wielu osobom lepszej przyszłości, albo sprawić, że społeczeństwo przyszłości będzie, jak twierdzi Erich Fromm, odczłowieczonym społeczeństwem technotronicznym[3].

1 Zob. M. Castells, *Społeczeństwo sieci*, PWN, Warszawa 2011.

2 J.D. Bolter, *Komputer: Maszyna i narzędzie*, [w:] *Nowe media w komunikacji społecznej XX wieku*, red. M. Hopfinger, Oficyna Naukowa, Warszawa 2002, s. 359.

3 H. Krauze-Sikorska, M. Klichowski, *Świat digital natives. Młodzież w poszukiwaniu siebie i innych*, Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza, Poznań 2013, s. 67.

Koniec XX wieku opisywano często przy użyciu takich określeń jak „rewolucja informatyczna" czy „rewolucja technologiczna" – zjawisk, które zmodyfikowały fundamenty współczesnych społeczeństw. Staliśmy się (lub wciąż stajemy) społeczeństwem informacyjnym, które nigdy nie przestało (i z pewnością nie przestanie) być „społeczeństwem ryzyka"[4]. Nowe technologie zmieniły relacje społeczne, ale także stworzyły nową – wirtualną – płaszczyznę dla rozwoju gospodarki. Jak twierdzi Piotr Sienkiewicz, jedną z niepożądanych, choć nieusuwalnych cech społeczeństwa informacyjnego jest obecność ryzyka cyberzagrożeń – rozumianego jako wzrost cyberprzestępczości i groźba cyberterroryzmu. Pisze także, iż na nową przyszłość powinniśmy spoglądać bardziej realistycznie: „optymizm technologiczny, towarzyszący przyspieszonemu postępowi naukowo-technicznemu w drugiej połowie XX wieku, obecnie ustępuje postawom sceptycznym wyrażającym częściej obawy i zwątpienie niż nadzieje na bezpieczny, trwały i zrównoważony rozwój cywilizacyjny"[5]. Ta nowa płaszczyzna stanowi obecnie, jak przekonuje inny badacz tej problematyki,

> pole dla nowych jakościowo zagrożeń. Wirtualna rzeczywistość, pozbawiona geograficznego parametru mierzalności, nie tylko przekracza kategorię terytorialności, ale przede wszystkim, za sprawą nieograniczonej sfery wolności słowa, uniemożliwia pełną kontrolę nad nadawcą, przekazem oraz odbiorcą. Złudne przekonanie o pełnej anonimowości powoduje, że nowy obszar ludzkiej działalności, pozbawiony tradycyjnej kontroli, sprawdzonej w świecie organicznym, staje się areną coraz chętniej wykorzystywaną przez cyberprzestępców[6].

Nie można również zapominać, że nowe zagrożenia mają wielowymiarowy charakter. Dotyczą zarówno bezpieczeństwa sfery pry-

4 W sensie używanym przez Ulricha Becka, zob. U. Beck, *Społeczeństwo ryzyka. W drodze do innej nowoczesności*, Wydawnictwo Naukowe Scholar, Warszawa 2002 oraz U. Beck, *Społeczeństwo światowego ryzyka. W poszukiwaniu utraconego bezpieczeństwa*, Wydawnictwo Naukowe Scholar, Warszawa 2012.

5 P. Sienkiewicz, *Media kształtujące społeczne wzburzenie*, [w:] *Media a opinie i postawy społeczne*, red. J. Bierówka, Z. Pucek, Krakowskie Towarzystwo Edukacyjne – Oficyna Wydawnicza AFM, Kraków 2011, s. 20–21.

6 M. Karatysz, *Zjawisko cyberprzestępczości a polityka cyberbezpieczeństwa w regulacjach prawnych Rady Europy, Unii Europejskiej i Polski*, „Refleksje" 2013, nr 7, s. 139.

watnej jednostek, jak i bezpieczeństwa państwa. Cyberprzestrzeń, o której mowa, stwarza nowe możliwości dla rozwoju podmiotów państwowych (pozapaństwowych) czy jednostek, ale jest również źródłem poważnych zagrożeń dla ich bezpieczeństwa[7]. Radosław Bania podkreśla, że „przestrzeń komputerowa staje się obszarem, w który zostają przenoszone różnego rodzaju konflikty i który jest w szczególności otwarty na różnego rodzaju ataki, skierowane nie tylko przeciwko osobom cywilnym, ale już w znacznej mierze przeciwko istotnym elementom infrastruktury krytycznej poszczególnych państw"[8]. Stąd potrzeba stałego poszerzania znaczeń takich pojęć, jak bezpieczeństwo czy zagrożenia[9]. Wielu ekspertów przyznaje jednak, że przede wszystkim permanentny postęp technologiczny znacząco utrudnia formułowanie jednoznacznych definicji tych terminów[10]. W literaturze można odnaleźć wiele bardzo szczegółowych typologii zagrożeń dla bezpieczeństwa w przestrzeni internetowej (cyberprzestępstw)[11]. Na potrzeby niniejszego artykułu – którego główną wartością jest analiza danych empirycznych – przyjęto definicję ogólną, która traktuje cyberprzestępstwa jako „grupę czynów zabronionych polegających na posługiwaniu się elektronicznymi systemami przetwarzania informacji do naruszania dóbr prawnych chronionych przez prawo

7 A. Żebrowski, *Bezpieczeństwo informacyjne Polski a walka informacyjna*, „Roczniki Kolegium Analiz Ekonomicznych" 2013, nr 29, s. 447. Zob. także: K. Liderman, *Bezpieczeństwo informacyjne,* PWN, Warszawa 2012, s. 17–26 oraz M. Plecka, A. Rychły-Lipińska, *Bezpieczeństwo informacyjne*, [w:] *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa*, red. A. Urbanek, Wydawnictwo Społeczno-Prawne, Słupsk 2013.

8 R. Bania, *Wojny w cyberprzestrzeni – przypadek Iranu*, [w:] *Bezpieczeństwo narodowe i międzynarodowe w regionie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*, red. R. Bania, K. Zdulski, Wydawnictwo Naukowe, Łódź 2012, s. 186.

9 J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Instytut Studiów Politycznych PAN, Warszawa 1996.

10 A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 32. Zob. także: M. Gercke*, Understanding Cybercrime: Phenomena, Challenges and Legal Response,* http://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf (dostęp: 10.02.2015).

11 Zob. S. Gordon, R. Ford, *On the definition and classification of cybercrime*, „Journal of Computer Virology" 2006, no. 2; M. Nowak, *Cybernetyczne przestępstwa – definicje i przepisy prawne*, „Biuletyn EBIB" 2010, nr 4, http://www.ebib.pl.

karne”[12]. Maciej Siwicki podkreśla, że ten rodzaj przestępczości dotyczy relatywnie szerokiego kręgu przestępstw, a mianowicie: (1) przestępstw przeciwko bezpieczeństwu przetwarzanej informacji, (2) przestępstw związanych z użyciem środków masowego przekazu do rozpowszechniania lub prezentowania informacji zakazanych przez prawo (tzw. przestępstwa związane z treścią informacji) oraz (3) pozostałych przestępstw instrumentalnego wykorzystania (użycia) elektronicznych sieci informatycznych i systemów informatycznych do naruszania dóbr prawnych, chronionych przez prawo karne[13].

Źródła danych i problematyka

W niniejszym artykule podjęto próbę zaprezentowania rezultatów analizy danych z badań nad europejską opinią publiczną w zakresie bezpieczeństwa cybernetycznego[14]. Z uwagi na charakter danych dokonano porównania, które pozwala na ten problem spojrzeć z uwzględnieniem zróżnicowania zarówno poczucia zagrożenia, świadomości zagrożenia, jak i zachowań ryzykownych w tym wymiarze oraz zachowań mających na celu zwiększenie indywidualnego bezpieczeństwa. Postawy społeczeństwa polskiego przedstawiono zatem na

12 M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo” 2012, nr 7–8, s. 241. Zob. także: M. Siwicki, *Cyberprzestępczość*, Wydawnictwo C.H.Beck, Warszawa 2013, s. 9–20.

13 M. Siwicki, *Podział…*, s. 250–251. Ciekawej perspektywy dostarczają także Brunon Hołyst i Jacek Pomykała, rozróżniając kategorię cyberprzestępstw dokonywanych z (rzeczywistym lub potencjalnym) użyciem przemocy oraz dokonywanych bez użycia przemocy. W ramach tej pierwszej wymieniają: cyberterroryzm, napaść przez zastraszenie, cyberprześladowanie oraz pornografię dziecięcą. W ramach drugiej: cyberwtargnięcia, cyberkradzieże, cyberoszustwa, cyberzniszczenia oraz inne cyberprzestępstwa; zob. B. Hołyst, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, „Prokuratura i Prawo” 2011, nr 1, s. 17–19.

14 Źródłem wiedzy wykorzystanej w artykule stały się wyniki badania Eurobarometr 79.4. Do analizy porównawczej wykorzystano właściwy zbiór danych zdeponowany w serwisie ZACAT, pozwalającym na wyszukiwanie, przeglądanie, analizę i pobieranie danych z badań społecznych, a dostarczanych przez niemiecki instytut badawczy GESIS (Leibniz-Institut für Sozialwissenschaften); European Commission, Brussels (2014): Eurobarometer 79.4 (2013). TNS Opinion, Brussels [producer]. GESIS Data Archive, Cologne. ZA5852 Data file Version 3.0.1.

tle postaw społeczności europejskiej (z 27 państw Unii Europejskiej[15]), a dodatkowo wyróżniono podział na zjawiska dominujące w społeczeństwach tzw. starej UE (15 państw tworzących Wspólnotę Europejską do 2004 roku[16]) oraz w społeczeństwach nowej UE (12 państw[17]). Taki podział należy uznać za funkcjonalny przede wszystkim ze względu na fakt, iż pozwala dostrzec różnice w aspekcie międzynarodowym na kilku płaszczyznach, m.in.

- w dostępie i sposobach wykorzystania nowych technologii;
- percepcji zagrożeń dla bezpieczeństwa w internecie;
- stanie nastrojów społecznych (obaw) w tym zakresie;
- sposobach zapobiegania zagrożeniom.

Dodatkowo, obserwacja analizowanych trendów w czasie prowadzi do wniosku, że społeczeństwa nowej UE (w tym polskie) będą raczej powielać wzory zachodnioeuropejskie.

W toku analizy sformułowano kilka ogólnych wniosków:

- widać różnice w formach aktywności podejmowanych w internecie (np. czy sieć służy tylko pozyskiwaniu informacji, czy jest także przestrzenią dla zachowań konsumenckich i biznesowych);
- charakter podejmowanych aktywności determinuje rodzaj i skalę zagrożeń i faktycznych (deklarowanych przez respondentów) aktów cyberprzestępczych;
- to z kolei implikuje różnice w zakresie i poziomie świadomości zagrożeń i deklarowanych obaw, ale także konkretnych zachowań na rzecz własnego bezpieczeństwa (np. zmiana haseł dostępu do serwisów internetowych).

Aktywność w internecie

Częstotliwość korzystania z internetu, jak również sposoby wykorzystania tego medium muszą determinować skalę zjawiska zwanego

15 W analizie nie uwzględniono danych dla Chorwacji, która jest państwem członkowskim UE od 1 lipca 2013 roku.

16 Austria, Belgia, Dania, Finlandia, Francja, Grecja, Hiszpania, Holandia, Irlandia, Luksemburg, Niemcy, Portugalia, Szwecja, Wielka Brytania, Włochy.

17 Bułgaria, Cypr, Czechy, Estonia, Litwa, Łotwa, Malta, Polska, Rumunia, Słowacja, Słowenia, Węgry.

„cyberprzestępczością". Warto zatem bliżej przyjrzeć się strukturze czasu poświęcanego na aktywność w internecie, z uwzględnieniem wspomnianego międzynarodowego zróżnicowania. Taka perspektywa ukazuje bowiem pewne istotne cechy dominujących wzorów zachowań na tym polu (tab. 1). Przede wszystkim należy zwrócić uwagę na swoisty kontrast między starą a nową UE. W pierwszym przypadku do korzystania z internetu przynajmniej raz dziennie przyznaje się większość populacji (58%, w tym aż 44% korzysta kilka razy dziennie). W drugim – mniej niż połowa, dokładnie 43%. Polskie społeczeństwo wpisuje się tutaj w tendencję właściwą dla całej nowej Unii. Widoczny jest również większy udział obywateli starej UE w ogólnym wskaźniku aktywności w internecie (UE 27: 54%). Opisane tu zjawisko w analogicznym stopniu dotyczy tzw. cyfrowego wykluczenia – nie tyle obiektywnego (brak dostępu do technologii i usług), co obecnego w zachowaniach (tj. faktycznym niekorzystaniu z technologii czy usług). O wiele więcej mieszkańców nowej UE (Polacy nie są tutaj wyjątkiem) przyznaje, że „nigdy" nie korzysta z internetu w takich celach, jak: korespondencja elektroniczna, pozyskiwanie informacji, komunikacja czy zakupy.

Tabela 1. Częstotliwość korzystania z internetu (%)

Jak często korzysta Pan(i) z internetu (np. by wysłać maile, poczytać wiadomości, porozmawiać ze znajomymi lub zrobić zakupy przez internet)?	POLSKA	UE STARA	UE NOWA	UE 27
Kilka razy dziennie / cały czas	33	44	31	41
Raz dziennie	11	14	12	13
Kilka razy w tygodniu	10	10	10	10
Raz w tygodniu	4	3	4	3
Kilka razy w miesiącu	2	1	2	1
Raz w miesiącu	1	1	1	1
Rzadziej	2	2	2	2
Nigdy	37	26	38	28
Trudno powiedzieć	1	1	1	1

Źródło: opracowanie własne na podstawie Eurobarometer 79.4.

Szczegółowe dane wskazują również na niejednolitość wzorów aktywności internetowej, która może być efektem zróżnicowania zasobności materialnej, ale i otwartości na nowe technologie (tab. 2). Typowy Polak korzysta z internetu głównie za pośrednictwem laptopa/netbooka (59%) oraz komputera stacjonarnego (52%)[18]. O wiele rzadziej natomiast używa do tego celu telefonu komórkowego (smartfona). Tym urządzeniem posługuje się co dziesiąty obywatel Polski (dokładnie 11%). Statystyczny mieszkaniec starej UE jest bardziej mobilny, częściej bowiem (niż mieszkańcy nowej UE) wykorzystuje takie urządzenia jak tablet czy właśnie smartfon. Także telewizor jako odbiornik internetu jest tam bardziej rozpowszechniony (7%). Widać zatem mniej tradycyjne wzory zachowań w społeczeństwach starej piętnastki.

Tabela 2. Typy urządzeń do korzystania z internetu (%)

Jakich urządzeń używa Pan(i) do korzystania z internetu?	POLSKA	UE STARA	UE NOWA	UE 27
Komputera stacjonarnego	52	51	62	53
Laptopa/netbooka	59	65	51	62
Tableta	5	16	5	14
Smartfona	11	39	14	35
Telewizora	3	7	2	6
Inne	0	1	0	1
Trudno powiedzieć	0	1	0	0

Źródło: opracowanie własne na podstawie Eurobarometer 79.4.

Powyższą tezę potwierdza także analiza danych dotyczących konkretnych czynności, które użytkownicy podejmują w internecie (tab. 3[19]). Okazuje się, że obywatele starej Unii częściej podejmują aktywności bardziej ryzykowne, gdzie akt cyberprzestępczy może mieć poważniejsze (np. materialne, finansowe) konsekwencje. Symbolicznym przykładem jest bankowość internetowa, z której usług korzysta ponad połowa (51%) mieszkańców tej części kontynentu i tylko 39%

18 Odsetki nie sumują się do 100, bowiem respondenci mogli wskazywać więcej niż jedno urządzenie służące do korzystania z internetu.

19 Pytanie zadano jedynie osobom, które wcześniej zadeklarowały, że kiedykolwiek korzystają z internetu.

obywateli nowej UE. Ci również zdecydowanie rzadziej wykorzystują sieć w celu zakupu towarów czy usług. W tym przypadku różnica między poziomem powszechności tej formy aktywności w starej i nowej UE jest jeszcze większa.

Tabela 3. Formy aktywności w internecie (%)

Które z poniższych czynności wykonuje Pan(i) w internecie?	POLSKA	UE STARA	UE NOWA	UE 27
Bankowość internetowa	50	51	39	48
Zakup towarów i usług (wakacje, książki, muzyka itp.)	39	54	35	50
Sprzedaż towarów i usług	11	20	11	18
Korzystanie z internetowych portali społecznościowych	52	53	55	53
Poczta elektroniczna	79	86	76	84
Czytanie wiadomości w internecie	83	57	73	60
Granie w gry za pośrednictwem internetu	21	27	27	27
Oglądanie telewizji	12	19	16	19
Inne	2	4	3	3
Żadne	1	1	2	1
Trudno powiedzieć	0	0	0	0

Źródło: opracowanie własne na podstawie Eurobarometer 79.4.

Poziom poinformowania w zakresie bezpieczeństwa cybernetycznego

Kolejnym ważnym wymiarem analizy, w świetle którego należy rozpatrywać problem bezpieczeństwa cybernetycznego we współczesnej Europie, jest kwestia stopnia poinformowania obywateli na temat rozmaitych zagrożeń w tej dziedzinie (tab. 4). W tym miejscu ujawniają się bowiem znaczące różnice. Otóż 52% obywateli całej UE deklaruje swoje niedoinformowanie w tym zakresie. Ta tendencja jest bardziej wyraźna w nowej części Wspólnoty (60%), choć także połowa populacji starej UE zgłasza braki w wiedzy na ten temat. Wydaje się więc konieczne podejmowanie większych wysiłków na rzecz szerzenia świadomości

różnych form zagrożeń w całej UE. Deficyt informacji stanowi bowiem główną przyczynę podejmowania ryzykownych aktywności.

Tabela 4. Stopień poinformowana o zagrożeniach w internecie (%)

Jak dobrze poinformowany(a) czuje się Pan(i) na temat zagrożeń związanych z cyberprzestępczością?	POLSKA	UE STARA	UE NOWA	UE 27
Bardzo dobrze poinformowany(a)	11	10	8	9
Raczej dobrze poinformowany(a)	31	37	28	35
Niezbyt dobrze poinformowany(a)	29	28	30	29
W ogóle nie poinformowany(a)	26	22	30	23
Trudno powiedzieć	3	4	5	4

Źródło: opracowanie własne na podstawie Eurobarometer 79.4.

Obywatele całej UE zdecydowanie przyznają, że posiadają odpowiednie umiejętności korzystania z internetu w zakresie takim jak bankowość internetowa czy dokonywanie zakupów (tab. 5). Taką pewność zgłasza 70% społeczeństw starej i 68% nowej Unii. Pewnym wyjątkiem – aczkolwiek w pozytywnym sensie – są tutaj Polacy, którzy jeszcze częściej stwierdzają posiadanie tychże umiejętności (aż 77%). Ta pewność siebie niestety – na co wskazywano w poprzednim wątku – nie łączy się z większym poziomem poinformowania, jeśli chodzi o potencjalne zagrożenia, bowiem aż 55% z nich wyraża opinię o niedostatecznym poinformowaniu w tej sprawie.

Tabela 5. Poziom umiejętności w zakresie korzystania z bankowości i zakupów przez internet (%)

Na ile jest Pan(i) pewny(a), że potrafi Pan(i) korzystać z internetu w zakresie takim jak bankowość internetowa lub zakupy przez internet?	POLSKA	UE STARA	UE NOWA	UE 27
Bardzo pewny(a)	30	27	27	27
Raczej pewny(a)	47	43	41	43
Niezbyt pewny(a)	14	17	16	17
W ogóle niepewny(a)	5	11	13	11
Trudno powiedzieć	3	1	4	2

Źródło: opracowanie własne na podstawie Eurobarometer 79.4.

Dynamiczny rozwój nowych technologii powoduje powstawanie i poszerzanie się luki kompetencyjnej w społeczeństwie. Ci, dla których nowe media stanowią część naturalnego środowiska, korzystają więcej i szybciej. To ich często określa się mianem *digital natives* (cyfrowi tubylcy)[20]. Przestrzeń internetu doświadcza jednak rozwarstwienia. Jak pisze Magdalena Szpunar, „dla jednych stanowiła będzie środowisko przyjazne, w którym zaspokajają niemal wszystkie swoje społeczne potrzeby, dla innych będzie *terra incognita* pełną zasadzek i trudności czyhających na niewytrawnego użytkownika"[21]. To jeszcze nie znaczy, że na zagrożenia w internecie wystawieni są tylko ci drudzy. Cyfrowi tubylcy narażeni są być może bardziej – z racji częstotliwości oraz form aktywności podejmowanych w internecie.

Poczucie zagrożenia cyberprzestępczością

Społeczne poczucie bezpieczeństwa jest konsekwencją zarówno obiektywnego stanu rzeczy, jak i subiektywnego przekonania jednostek, które może być determinowane rozmaitymi bodźcami o charakterze racjonalnym i – być może częściej – emocjonalnym. W praktyce jego wskaźnikiem jest poziom oraz zakres obaw, jakie towarzyszą obywatelom – użytkownikom internetu. W tabeli 6 zestawiono wyniki dotyczące obaw, z jakimi mieszkańcy UE wiążą różne formy wirtualnej aktywności. Wśród nich wyróżniono:

- kradzież tożsamości;
- próby wyłudzenia danych osobowych (loginów, haseł);
- oszustwo internetowe (w procesie sprzedaży internetowej);
- przypadkowe natknięcie się na treści związane z pornografią dziecięcą;
- przypadkowe natknięcie się na treści promujące nienawiść lub ekstremizm religijny;

20 Zob. M. Prensky, *Digital Natives, Digital Immigrants*, „On the Horizon" 2001, Vol. 9, No. 5. J. Katz z kolei pisze o „cyfrowych obywatelach", zob. J. Katz, *The Digital Citizen*, „Wired" 1997, No. 12.

21 M. Szpunar, *Przestrzeń Internetu – nowy wymiar przestrzeni społecznej*, [w:] *Od robotnika do internauty. W kierunku społeczeństwa informacyjnego*, red. A. Siwik, L. Haber, AGH Uczelniane Wydawnictwa Naukowo-Dydaktyczne, Kraków 2008, s. 227.

- niedostępność usług internetowych z powodu „cyberataku";
- atak hakerski na konto (mailowe, w portalu społecznościowym);
- oszustwo internetowe (w zakresie bankowości internetowej).

Tabela 6. Obawy związane z aktywnością w internecie (%)

Na ile zaniepokojony(a) jest Pan(i) osobiście tym, że może doświadczyć lub zostać ofiarą następujących cyberprzestępstw?				
	POLSKA	UE STARA	UE NOWA	UE 27
Kradzież tożsamości (ktoś kradnie Pana(i) dane osobowe i podaje się za Pana(ią), np. robi zakupy posługując się Pana(i) imieniem i nazwiskiem)				
Bardzo zaniepokojony(a)	19	17	20	17
Raczej zaniepokojony(a)	36	34	35	34
Raczej niezaniepokojony(a)	30	33	29	32
W ogóle niezaniepokojony(a)	12	15	13	15
Trudno powiedzieć	3	1	2	1
Otrzymywanie od oszustów e-maili lub telefonów z prośbą o udostępnienie Pana(i) komputera, danych logowania lub danych osobowych (w tym danych bankowych lub płatniczych)				
Bardzo zaniepokojony(a)	13	13	14	13
Raczej zaniepokojony(a)	37	29	34	30
Raczej niezaniepokojony(a)	35	39	34	38
W ogóle niezaniepokojony(a)	12	18	17	18
Trudno powiedzieć	3	1	3	1
Oszustwo internetowe, w którym zakupione towary nie zostały dostarczone, były podrobione lub niezgodne z opisem				
Bardzo zaniepokojony(a)	12	10	14	11
Raczej zaniepokojony(a)	39	30	35	31
Raczej niezaniepokojony(a)	35	39	31	37
W ogóle niezaniepokojony(a)	12	20	17	19
Trudno powiedzieć	4	1	3	2
Przypadkowe natknięcie się w internecie na pornografię dziecięcą				
Bardzo zaniepokojony(a)	17	19	18	19
Raczej zaniepokojony(a)	33	24	30	25
Raczej niezaniepokojony(a)	32	34	30	34
W ogóle niezaniepokojony(a)	14	22	18	21
Trudno powiedzieć	4	1	4	2

Przypadkowe natknięcie się na materiały, które promują nienawiść rasową lub ekstremizm religijny				
Bardzo zaniepokojony(a)	9	10	9	10
Raczej zaniepokojony(a)	33	24	30	25
Raczej niezaniepokojony(a)	37	42	37	41
W ogóle niezaniepokojony(a)	17	24	21	23
Trudno powiedzieć	4	1	4	2
Brak możliwości uzyskania dostępu do usług internetowych (np. usług bankowych) z powodu ataku cybernetycznego				
Bardzo zaniepokojony(a)	11	10	12	10
Raczej zaniepokojony(a)	34	26	31	27
Raczej niezaniepokojony(a)	37	42	34	40
W ogóle niezaniepokojony(a)	14	21	19	20
Trudno powiedzieć	5	2	5	2
Atak hakerski na Pana(i) konto w mediach społecznościowych lub konto poczty elektronicznej				
Bardzo zaniepokojony(a)	12	13	15	13
Raczej zaniepokojony(a)	34	32	33	32
Raczej niezaniepokojony(a)	35	37	32	36
W ogóle niezaniepokojony(a)	14	18	17	18
Trudno powiedzieć	4	1	4	2
Padnięcie ofiarą oszustwa internetowego dotyczącego karty kredytowej lub bankowości				
Bardzo zaniepokojony(a)	15	18	19	18
Raczej zaniepokojony(a)	36	31	32	31
Raczej niezaniepokojony(a)	35	33	30	32
W ogóle niezaniepokojony(a)	11	18	16	17
Trudno powiedzieć	3	1	3	2

Źródło: opracowanie własne na podstawie Eurobarometer 79.4.

Szczegółowe dane zaprezentowane w tabeli 6 można podsumować kilkoma ogólnymi spostrzeżeniami. O ile różnice w poziomie obaw w społeczeństwach starej i nowej UE nie są znaczące, o tyle warto dostrzec kilka interesujących dysproporcji. Po pierwsze, w każdym z badanych wymiarów obawy mieszkańców nowej części UE są większe. Oznacza to, że lęk przed doświadczeniem przejawów cyberprze-

stępczości (w jakiejkolwiek postaci) dotyczy w większym stopniu tych populacji, w których poziom poinformowania o tego rodzaju zagrożeniach jest mniejszy. Najbardziej istotne różnice również dotyczą tych form internetowej aktywności, które w nierównomierny sposób dominują w starej i nowej części Wspólnoty. Chodzi przede wszystkim o zakupy przez internet (obawy w starej UE na poziomie 40%, w nowej – 48%) oraz bankowość internetową (stara UE: 36%, nowa UE: 43%). Jak wcześniej wspominano, są to te formy wykorzystania sieci, z których częściej korzystają mieszkańcy starej Unii. Widoczny jest więc związek między częstotliwością wykorzystania określonych narzędzi a stopniem poinformowania o zagrożeniach oraz poziomem obaw związanych z potencjalnym atakiem. Jeśli natomiast chodzi o społeczeństwo polskie, to w dużej mierze powiela ono trendy właściwe dla wskaźnika ogólnego dla państw nowej UE (w każdym z wymiarów odchylenia wynoszą maksymalnie +/- 3%[22]).

Pośród szczegółowo opisanych obaw w zakresie zakupów oraz bankowości internetowej współcześni Europejczycy wymieniają przede wszystkim: możliwość utraty tożsamości (ktoś może wejść w posiadanie moich danych osobowych) – 37% dla całej UE, obawy co do bezpieczeństwa płatności przez internet (35%) czy niemożność sprawdzenia produktu lub dopytania o jego cechy (24%). Mniej, bo tylko 15%, obawia się nieotrzymania zakupionych produktów lub usług. Jednocześnie 23% obywateli UE przyznaje, że żadnych obaw nie posiada. Potwierdzenie tych danych znajduje się również w rozkładach odpowiedzi na pytanie o odpowiedzialność poszczególnych podmiotów za ochronę danych w internecie. 70% mieszkańców wszystkich 27 państw UE uważa, że „dane osobowe w internecie nie są chronione przez strony internetowe", a 64% – że „nie są chronione przez władze publiczne".

Warto w tym kontekście postawić pytanie o to, w jakim stopniu określone obawy wpływają na ludzkie zachowania zorientowane na zwiększenie bezpieczeństwa. Dobrym wskaźnikiem są odpowiedzi respondentów Eurobarometru na pytanie: „Czy obawy związane z kwestiami bezpieczeństwa skłoniły Pana(ią) do zmiany sposobu korzystania z internetu w jakikolwiek z następujących sposobów?" (tab. 7).

22 Po zsumowaniu odpowiedzi: „Bardzo zaniepokojony(a)" oraz „Raczej zaniepokojony(a)".

Tabela 7. Sposoby zapobiegania atakom w internecie (%)

Czy obawy związane z kwestiami bezpieczeństwa skłoniły Pana(ią) do zmiany sposobu korzystania z internetu w jakikolwiek z następujących sposobów?	POLSKA	UE STARA	UE NOWA	UE 27
Mniej chętne kupowanie towarów przez internet	11	17	16	17
Mniej chętne korzystanie z bankowości internetowej	9	15	12	15
Mniej chętne udostępnianie danych osobowych na stronach internetowych	19	37	23	34
Zmiana ustawień bezpieczeństwa (np. przeglądarka, media społecznościowe, wyszukiwarka)	9	18	10	16
Odwiedzanie tylko znanych i zaufanych stron internetowych	21	33	28	32
Korzystanie z różnych haseł dla różnych stron	17	26	17	24
Nieotwieranie e-maili od nieznajomych	20	43	29	40
Korzystanie tylko z własnego komputera	17	26	25	26
Zainstalowanie oprogramowania antywirusowego	22	49	33	46
Anulowanie zakupu w internecie ze względu na podejrzenia co do sprzedawcy lub strony internetowej	4	6	3	6
Inne	1	1	1	1
Żadne	30	16	23	18
Trudno powiedzieć	9	1	4	2

Źródło: opracowanie własne na podstawie Eurobarometer 79.4.

Pośród najczęściej stosowanych zachowań prewencyjnych znajdują się: instalacja programu antywirusowego, nieotwieranie wiadomości elektronicznych od nieznajomych, rzadsze udostępnianie danych osobowych w internecie oraz odwiedzanie głównie znanych i zaufanych stron internetowych (hierarchia dla UE 27). Do refleksji natomiast powinny skłaniać odsetki wskazań na poszczególne zachowania

Polaków (niższe od średniej europejskiej) oraz fakt, że statystycznie 18% obywateli UE nie podejmuje żadnych działań służących zwiększeniu bezpieczeństwa w internecie. Polacy wyraźnie zawyżają tę średnią, okazuje się bowiem, że niemal co trzeci z nas w żaden sposób nie zmienił sposobu korzystania z internetu, mimo obaw, które posiada.

Skala zjawiska

Problem bezpieczeństwa trzeba zwykle rozpatrywać na dwóch płaszczyznach: subiektywnej oraz obiektywnej. Z jednej strony interesuje nas społeczne (często zindywidualizowane) poczucie istnienia zagrożenia lub jego braku, z drugiej – rzeczywisty brak lub obecność zagrożeń[23]. W pierwszym przypadku należy pamiętać, że poziom poczucia bezpieczeństwa (mierzony np. poprzez analizę obaw zgłaszanych przez obywateli) nie zawsze odzwierciedla rzeczywiste zagrożenie[24]. To z kolei można próbować opisać na podstawie danych z tabeli 8.

Okazuje się, że najczęstszą formą cyberprzestępczości, z którą spotkali się dotąd mieszkańcy Unii Europejskiej, jest otrzymywanie od oszustów e-maili lub telefonów z prośbą o udostępnienie komputera, danych logowania lub danych osobowych (w tym danych bankowych lub płatniczych). Niemal jedna trzecia z nich (32%) przyznaje, że zdarzyło im się to w przeszłości (przy czym 7% podkreśla, że często

23 R. Zięba, *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych*, [w:] *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, red. D.B. Bobrow, E. Haliżak, R. Zięba, Wydawnictwo Naukowe Scholar, Warszawa 1997, s. 5–6. Por. M.Z. Kulisz, *Proces planowania bezpieczeństwa państwa w okresie transformacji ustrojowej*, Zakład Wydawnictw Statystycznych, Radom 2007, s. 9 oraz E. Moczuk, *Społeczne poczucie bezpieczeństwa mieszkańców społeczności lokalnej*, [w:] *Samorząd a policja. Kształtowanie bezpieczeństwa lokalnego*, red. A. Szymaniak, Wydawnictwo Naukowe Instytutu Nauk Politycznych i Dziennikarstwa Uniwersytetu im. Adama Mickiewicza, Poznań 2007, s. 165 i nast.

24 R. Marzęcki, *Poczucie bezpieczeństwa i potrzeba demokratycznego dialogu w epoce społeczeństwa ryzyka*, [w:] *Bezpieczeństwo RP: wczoraj i dziś. Studia z zakresu bezpieczeństwa państwa*, red. M. Śliwa, A. Żebrowski, R. Kłaczyński, Wydawnictwo Naukowe UP, Kraków 2014, s. 251. Zob. także: P. Pieńkowski, *Społeczna percepcja bezpieczeństwa jako czynnik geopolityczny*, [w:] *Geopolityka. Elementy teorii, wybrane metody i badania*, red. Z. Lach, J. Wendt, Instytut Geopolityki, Częstochowa 2010, s. 49.

padało ofiarą takiego działania). Ponad dwa razy rzadziej (14%) typowy Europejczyk natyka się w internecie na materiały, które promują nienawiść rasową lub ekstremizm religijny. 12% natomiast twierdzi, że padło ofiarą ataku hakerskiego na konto w mediach społecznościowych lub konto poczty elektronicznej, a także, że utraciło dostęp do usług internetowych (np. usług bankowych) w wyniku ataku cybernetycznego. Co dziesiąty (10%) obywatel UE został przynajmniej raz oszukany przy zakupach przez internet (zakupione towary nie zostały dostarczone, były podrobione lub niezgodne z opisem). Z kolei najrzadziej (7% takich wskazań) zdarzały się akty kradzieży tożsamości oraz bezprawne wykorzystanie czyjejś karty kredytowej lub włamanie do systemu bankowości internetowej.

Tabela 8. Przypadki działalności cyberprzestępczej wobec mieszkańców UE (%)

Cyberprzestępczość może obejmować wiele różnych rodzajów działalności przestępczej. Jak często doświadczał(a) Pan(i) lub był(a) Pan(i) ofiarą następujących sytuacji?				
	POLSKA	UE STARA	UE NOWA	UE 27
Kradzież tożsamości (ktoś kradnie Pana(i) dane osobowe i podaje się za Pana(ią), np. robi zakupy posługując się Pana(i) imieniem i nazwiskiem)				
Często	2	1	1	1
Rzadko	6	6	5	6
Nigdy	91	93	93	93
Trudno powiedzieć	2	1	2	1
Otrzymywanie od oszustów e-maili lub telefonów z prośbą o udostępnienie Pana(i) komputera, danych logowania lub danych osobowych (w tym danych bankowych lub płatniczych)				
Często	3	8	2	7
Rzadko	14	27	16	25
Nigdy	81	65	81	68
Trudno powiedzieć	2	1	1	1
Oszustwo internetowe, w którym zakupione towary nie zostały dostarczone, były podrobione lub niezgodne z opisem				
Często	2	1	1	1
Rzadko	11	10	9	9
Nigdy	86	89	88	89
Trudno powiedzieć	2	1	2	1

Przypadkowe natknięcie się na materiały, które promują nienawiść rasową lub ekstremizm religijny				
Często	3	2	2	2
Rzadko	12	12	14	12
Nigdy	83	85	82	85
Trudno powiedzieć	2	1	2	1
Brak możliwości uzyskania dostępu do usług internetowych (np. usług bankowych) z powodu ataku cybernetycznego				
Często	1	1	1	1
Rzadko	7	12	8	11
Nigdy	90	86	89	87
Trudno powiedzieć	2	1	3	2
Atak hakerski na Pana(i) konto w mediach społecznościowych lub konto poczty elektronicznej				
Często	1	1	1	1
Rzadko	7	11	8	11
Nigdy	89	86	89	87
Trudno powiedzieć	2	1	2	2
Padnięcie ofiarą oszustwa internetowego dotyczącego karty kredytowej lub bankowości				
Często	1	1	1	1
Rzadko	5	7	4	6
Nigdy	92	92	94	92
Trudno powiedzieć	1	1	1	1

Źródło: opracowanie własne na podstawie Eurobarometer 79.4.

Wracając do problemu bezpieczeństwa rozumianego w sensie subiektywnym (odczuwanego jako poczucie bezpieczeństwa lub jego braku), warto pamiętać, że jest ono w dużej mierze konstruowane społecznie oraz intersubiektywne[25]. Wielu autorów zwraca uwagę na zmienność i subiektywność rzeczywistości społecznej, a także na rolę czynników kulturowych i języka w kształtowaniu poczucia zagrożenia[26]. Ważnym narzędziem kreowania określonych stanów psychicznych

25 B. Buzan, O. Waever, J. de Wilde, *Security. A New Framework to Analysis*, Lynne Rienner Publishers, Boulder 1998, s. 24–26, 57.

26 J. Szulecka, K. Szulecki, *'Environmental Peacebuilding'. Transnarodowe działania na rzecz ochrony środowiska jako platforma zaawansowanego zapobiegania konfliktom na*

społeczeństwa są debaty publiczne toczone za pośrednictwem środków masowego komunikowania. Odpowiednio moderowane (przez ekspertów, polityków oraz dziennikarzy i publicystów) mogą spełniać użyteczne społecznie funkcje o charakterze informacyjnym, edukacyjnym czy socjalizacyjnym. W ten sposób powinny determinować wyższy stopień poinformowania w zakresie problematyki bezpieczeństwa wśród obywateli. Przytaczane wcześniej wyniki badań świadczą jednak o słabej jakości (często w ogóle braku) tego rodzaju debat i dyskusji na tematy związane z bezpieczeństwem cybernetycznym.

Podsumowanie

Dynamiczny rozwój współczesnych społeczeństw we wszystkich możliwych aspektach powoduje, że kurczą się nasze możliwości trafnego i skutecznego prognozowania przyszłych wydarzeń. Teraźniejszość – opisywana jako „płynna ponowoczesność" – dostarcza bowiem wielu problemów w opisie tego, co „tu i teraz". Wyzwaniem współczesności stają się nowe przestrzenie, które oferują, ale i narzucają inne zasady funkcjonowania państwa, gospodarki i społeczeństwa. Jednym z takich pól jest tzw. cyberprzestrzeń, która stanowi obietnicę nowych możliwości, ale jednocześnie generuje nowe zagrożenia. W wirtualnym świecie, choć ofiarą padają podmioty polityczne czy gospodarcze, najbardziej bezbronni wydają się zwykli obywatele – użytkownicy internetu, a więc medium, z którego na co dzień korzysta ponad połowa unijnej populacji. Zaprezentowane w artykule dane empiryczne ukazują dosyć wyraźny podział między państwami starej i nowej UE. Obywatele starej piętnastki są w większym stopniu mobilni (częściej używają tabletów/smartfonów do korzystania z internetu), a także częściej wykorzystują globalną sieć do podejmowania działalności konsumenckiej czy gospodarczej (bankowość internetowa oraz zakupy/sprzedaż w internecie). Istotnym problemem w tym kontekście staje się jednak poziom poinformowania obywateli całej UE na temat zagrożeń, jakie „czyhają" w cyberprzestrzeni. Ponad połowa deklaruje niedostateczny stopień poinformowania w tej kwestii, przy czym więcej takich osób

Bliskim Wschodzie, [w:] *Zaawansowane zapobieganie konfliktom*, red. W. Kostecki, Oficyna Wydawnicza ASPRA-JR, Warszawa 2011, s. 210.

mieszka w nowej części Unii. Okazuje się, że lęk przed doświadczeniem przejawów cyberprzestępczości dotyczy w większym stopniu tych populacji, gdzie również poziom poinformowania o tego rodzaju zagrożeniach jest mniejszy. Natomiast najbardziej zastanawiające są dane wskazujące na niepodejmowanie żadnych działań, których celem miałoby być zwiększenie bezpieczeństwa w sensie indywidualnym. Bierność w tym zakresie wykazuje prawie jedna piąta obywateli całej UE (o wiele więcej w nowej UE).

Bibliografia

Adamski A., *Prawo karne komputerowe*, Wydawnictwo C.H.Beck, Warszawa 2000.

Bania R., *Wojny w cyberprzestrzeni – przypadek Iranu*, [w:] *Bezpieczeństwo narodowe i międzynarodowe w regionie Bliskiego Wschodu i Północnej Afryki (MENA) u progu XXI wieku*, red. R. Bania, K. Zdulski, Wydawnictwo Naukowe, Łódź 2012.

Beck U., *Społeczeństwo ryzyka. W drodze do innej nowoczesności,* Wydawnictwo Naukowe Scholar, Warszawa 2002.

Beck U., *Społeczeństwo światowego ryzyka. W poszukiwaniu utraconego bezpieczeństwa*, Wydawnictwo Naukowe Scholar, Warszawa 2012.

Bolter J.D., *Komputer: Maszyna i narzędzie*, [w:] *Nowe media w komunikacji społecznej XX wieku,* red. M. Hopfinger, Oficyna Naukowa, Warszawa 2002.

Buzan B., Waever O., de Wilde J., *Security. A New Framework to Analysis*, Lynne Rienner Publishers, Boulder 1998.

Castells M., *Społeczeństwo sieci*, PWN, Warszawa 2011.

Eurobarometer 79.4 (2013). TNS Opinion, Brussels [producer]. GESIS Data Archive, Cologne. ZA5852 Data file Version 3.0.1.

Gercke M., *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* 2014, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf (dostęp: 10.02.2015).

Gordon S., Ford R., *On the definition and classification of cybercrime*, „Journal of Computer Virology" 2006, No. 2.

Hołyst B., Pomykała J., *Cyberprzestępczość, ochrona informacji i kryptologia*, „Prokuratura i Prawo" 2011, nr 1.

Karatysz M., *Zjawisko cyberprzestępczości a polityka cyberbezpieczeństwa w regulacjach prawnych Rady Europy, Unii Europejskiej i Polski*, „Refleksje" 2013, nr 7.

Katz J., *The Digital Citizen*, „Wired" 1997, No. 12.

Krauze-Sikorska H., Klichowski M., *Świat digital natives. Młodzież w poszukiwaniu siebie i innych*, Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza, Poznań 2013.

Kulisz M.Z., *Proces planowania bezpieczeństwa państwa w okresie transformacji ustrojowej,* Zakład Wydawnictw Statystycznych, Radom 2007.

Liderman K., *Bezpieczeństwo informacyjne,* PWN, Warszawa 2012.

Marzęcki R., *Poczucie bezpieczeństwa i potrzeba demokratycznego dialogu w epoce społeczeństwa ryzyka*, [w:] *Bezpieczeństwo RP: wczoraj i dziś. Studia z zakresu bezpieczeństwa państwa*, red. M. Śliwa, A. Żebrowski, R. Kłaczyński, Wydawnictwo Naukowe UP, Kraków 2014.

Moczuk E., *Społeczne poczucie bezpieczeństwa mieszkańców społeczności lokalnej*, [w:] *Samorząd a policja. Kształtowanie bezpieczeństwa lokalnego,* red. A. Szymaniak, Wydawnictwo Naukowe Instytutu Nauk Politycznych i Dziennikarstwa Uniwersytetu im. Adama Mickiewicza, Poznań 2007.

Nowak M., *Cybernetyczne przestępstwa – definicje i przepisy prawne*, „Biuletyn EBIB" 2010, nr 4, http://www.ebib.pl.

Pieńkowski P. (2010), *Społeczna percepcja bezpieczeństwa jako czynnik geopolityczny*, [w:] *Geopolityka. Elementy teorii, wybrane metody i badania,* red. Z. Lach, J. Wendt, Instytut Geopolityki, Częstochowa.

Plecka M., Rychły-Lipińska A. (2013). *Bezpieczeństwo informacyjne*, [w:] *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa,* red. A. Urbanek, Wydawnictwo Społeczno-Prawne, Słupsk.

Prensky M., *Digital Natives, Digital Immigrants*, „On the Horizon" 2001, Vol. 9, No. 5.

Sienkiewicz P., *Media kształtujące społeczne wzburzenie*, [w:] *Media a opinie i postawy społeczne,* red. J. Bierówka, Z. Pucek, Krakowskie Towarzystwo Edukacyjne – Oficyna Wydawnicza AFM, Kraków 2011.

Siwicki M., *Cyberprzestępczość,* Wydawnictwo C.H.Beck, Warszawa 2013.

Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8.

Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Instytut Studiów Politycznych PAN, Warszawa 1996.

Szpunar M., *Przestrzeń Internetu – nowy wymiar przestrzeni społecznej*, [w:] *Od robotnika do internauty. W kierunku społeczeństwa informacyjnego,* red. A. Siwik, L. Haber, AGH Uczelniane Wydawnictwa Naukowo-Dydaktyczne, Kraków 2008.

Szulecka J., Szulecki K., *'Environmental Peacebuilding'. Transnarodowe działania na rzecz ochrony środowiska jako platforma zaawansowanego zapobiegania konfliktom na Bliskim Wschodzie*, [w:] *Zaawansowane zapobieganie*

konfliktom, red. W. Kostecki, Oficyna Wydawnicza ASPRA-JR, Warszawa 2011.
Zięba R., *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych*, [w:] *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku,* red. D.B. Bobrow, E. Haliżak, R. Zięba, Wydawnictwo Naukowe Scholar, Warszawa 1997.
Żebrowski A., *Bezpieczeństwo informacyjne Polski a walka informacyjna*, „Roczniki Kolegium Analiz Ekonomicznych" 2013, nr 29.

Streszczenie

Wyzwaniem współczesności stają się nowe przestrzenie, które oferują, ale i narzucają inne zasady funkcjonowania państwa, gospodarki i społeczeństwa. Jednym z takich pól jest tzw. cyberprzestrzeń, która stanowi obietnicę nowych możliwości, ale jednocześnie generuje nowe zagrożenia. W niniejszym artykule podjęto próbę zaprezentowania rezultatów analizy danych z badań nad europejską opinią publiczną w zakresie bezpieczeństwa cybernetycznego. Dane na temat postaw społecznych zostały porównane między „starymi" i „nowymi" państwami Unii Europejskiej.

The Sense of Cybercrime Threat. International Variety

Abstract

New spaces that offer and impose distinct rules for functioning of the state, economy and society establish an important challenge for contemporary times. One of these fields is a "cyberspace", which gives us a lot of possibilities for development, but at the same time it generates new threats. In his article, the author presents results of the data analysis on European public opinion in the range of cyber security. The social attitudes data of an "old" member states of the European Union were compared with the social attitudes of "new" ones.