Cyberbezpieczeństwo, to w ostatnich czasach kluczowe słowo zajmujące znaczące miejsce w obszarze bezpieczeństwa. Spowodowała to rewolucja technologiczna i związany z nią wzrost naruszeń bezpieczeństwa informacji. Cyberbezpieczeństwo powinno spajać trzy podstawowe atrybuty bezpieczeństwa informacji, do których należą integralność, poufność i dostępność. Poufność informacji oznacza, że dane będą dostępne tylko osobom upoważnionym. Integralność (lub poprawność) określa, że informacja zapisana w systemie teleinformatycznym będzie odzwierciedlać faktyczny stan rzeczy. Wreszcie dostępność gwarantuje, że użytkownik mający prawo do korzystania z danej informacji, będzie posiadał do nich wgląd wtedy, gdy będą mu one potrzebne. Zachowując powyższe atrybuty, można zakładać, że cyberprzestrzeń, z której korzystamy na co dzień, często bez świadomości jej istnienia, jest względnie bezpieczna.

Cyberbezpieczeństwo to proces, który musi być nie tylko doskonalony, ale również ciągle modyfikowany w zależności od pojawiających się zagrożeń. Raporty przedstawiane przez różne organizacje, a także prezentowane analizy oraz doniesienia medialne wskazują,
iż cyberzagrożenia są najbardziej nieprzewidywalnym sposobem oddziaływania cyberprzestępców na funkcjonowanie państwa i jego obywateli. Funkcjonowanie społeczeństwa posiadającego wiedzę zakresu zagrożeń w cyberprzestrzeni jest wyjątkowo istotne z punktu widzenia bezpieczeństwa kraju. „Najsłabsze ogniwo” w cyfrowym świecie, jakim jest człowiek, a w przypadku cyberprzestrzeni - użytkownik końcowy, stanowi odnośnik do całości działań, polityk, procedur realizowanych przez państwo oraz podmioty do tego wyznaczone.

Główną rolę w procesie przygotowania społeczeństwa do świadomego i bezpiecznego korzystania z cyberprzestrzeni winien ponosić system edukacyjny. Zostało to zauważone i wyeksponowane w  *Rządowym programie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2008-2011*. Zaakceptowany w październiku 2008 roku ww. program był pierwszym dokumentem o tej randze, obejmującym zagadnienia bezpieczeństwa przestrzeni cybernetycznej państwa. Oddzielny rozdział w cytowanym dokumencie, został poświęcony edukacji społecznej i specjalistycznej, gdzie za realizację programów kształcenia
w uczelniach wyższych oraz kształcenia ustawicznego specjalistów odpowiadało Ministerstwo Edukacji Narodowej. Kampanie społeczne o charakterze edukacyjno-prewencyjnym miały stanowić podstawę informowania i edukowania społeczeństwa.
W czerwcu 2010 roku została zatwierdzona kolejna edycja programu pod nazwą *Rządowy program ochrony cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016*. Dokument ten pełnił rolę uzupełnienia poprzedniego programu i był wyznacznikiem trendów w obszarze geopolitycznym, dotyczącym cyberprzestrzeni i zagrożeń w niej występujących. Samo wprowadzenie do dokumentu opisuje problem ciągłej wojny w cyberprzestrzeni. Jednocześnie, dokument stał się propozycją działań prawnych, organizacyjnych, technicznych i edukacyjnych, których zastosowanie miało zwiększyć bezpieczeństwo oraz wzmocnić odporność infrastruktury teleinformatycznej na zagrożenia płynące ze strony cyberprzestrzeni. W programie określony został cel strategiczny, rozumiany jako zapewnienie ciągłego bezpieczeństwa państwa. Trudno zatem się nie zgodzić, iż jego osiągnięcie mogło być zrealizowane poprzez stworzenie podstaw prawnych, organizacyjnych oraz skoordynowanie informacji pomiędzy administracją publiczną oraz innymi użytkownikami cyberprzestrzeni. Zakładano, że cel programu osiągnie się poprzez realizację zadań szczegółowych, a jednym z nich było zwiększenie świadomości użytkowników, w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni. Miało to być realizowane poprzez edukację społeczną oraz specjalistyczną edukację z zakresu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej. Za realizację programu, zgodnie z kompetencjami odnośnie edukacji, odpowiadać miało, podobnie jak w pierwszej edycji programu, Ministerstwo Edukacji Narodowej. W programie zawarto szczegółowe wytyczne dla ministra w aspekcie szkolenia pełnomocników do spraw ochrony informacji niejawnej, racjonalizacji programów kształcenia w uczelniach wyższych, kształcenia kadry urzędniczej oraz ustanowienia dodatkowych kryteriów obsady stanowisk
w administracji publicznej i prowadzenia kampanii społecznej o charakterze edukacyjno-prewencyjnym. *Rządowy program ochrony cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016* spowodował, iż Ministerstwo Edukacji Narodowej otrzymało zadanie propagowania zmian w obszarze programów nauczania, które miały w konsekwencji ich realizacji doprowadzić do pozyskania wysoko wykwalifikowanych i przygotowanych kadr. Projekt wymagał zaangażowania szkół wyższych w program ochrony cyberprzestrzeni i dopasowania do nich ich programów nauczania. Rządowy dokument kładł nacisk na objęcie bezpieczeństwa cyberprzestrzeni długofalowym programem kierunków zamawianych, a także ustanowienie adekwatnego programu rozwoju kadry naukowej.

Ostatni element programu stanowiła kampania społeczna o  charakterze edukacyjno-prewencyjnym. Celem jej miało być podniesienie świadomości obywateli Rzeczypospolitej Polskiej, działających w obszarze cyberprzestrzeni. Program miał w zakresie edukacji społeczeństwa uświadamiać o zagrożeniach wynikających z  użytkowania cyberprzestrzeni. Świadomość oraz wiedza społeczeństwa w efekcie realizacji programu miała pozwolić
na ograniczenie ryzyka, wynikającego z pojawiających się zagrożeń w cyberświecie. Autorzy programu stwierdzali, *(…) iż kampania społeczna o charakterze edukacyjno-prewencyjnym stanowi wyzwanie i jest istotnym jego elementem (…)*. Podkreślenia wymaga, fakt, iż miała mieć charakter wielowymiarowy, tak by dotrzeć do szeregu zainteresowanych grup społecznych, a w szczególności do instytucji publicznych, przedsiębiorców, organizacji społecznych, jak i  użytkowników indywidualnych. Zakładała, że kampania będzie długofalowa i powszechna. Autorzy zalecali, by była skierowana głównie do dzieci, młodzieży, rodziców i nauczycieli.

Nauka o zagrożeniach, adresowana do dzieci, młodzieży i rodziców w dużej mierze miała być realizowana w placówkach oświatowych wszystkich szczebli. Załącznik numer 8 do programu opisuje szczegółowe jego założenia. W ramach działania programu, uczelnie wyższe powinny podnieść wiedzę kadry i studentów w obszarze cyberbezpieczeństwa. Realizować to miały poprzez uaktualnienie programów kształcenia ze szczególnym uwzględnieniem:

* *(…)przepisów prawa związanych z ochroną cyberprzestrzeni, ściganiem cyberterroryzmu i cyberprzestępstw,*
* *funkcji i zadań realizowanych przez jednostki odpowiedzialne za ochronę cyberprzestrzeni, na przykład CERT[[1]](#footnote-1)-y,*
* *norm i standardów związanych z bezpieczeństwem w cyberprzestrzeni,*
* *zasad zarządzania bezpieczeństwem w cyberprzestrzeni,*
* *polityki bezpieczeństwa teleinformatycznego,*
* *polityki bezpieczeństwa oraz procedur ochrony informacji i zasobów,*
* *identyfikacji zagrożeń,*
* *analiz ryzyka występujących w cyberprzestrzeni,*
* *skutków przełamania zabezpieczeń przez cyberprzestępców,*
* *procedur postępowania na wypadek ataku,*
* *procedur zgłaszania incydentów bezpieczeństwa,*
* *metod bezpiecznego korzystania z zasobów cyberprzestrzeni,*
* *sposobów i miejsc poszukiwania w sieci informacji dotyczących bezpieczeństwa (…)*.

Powyższe przykłady stanowiły podstawę tworzonych programów kształcenia
z zakresu cyberbezpieczeństwa, realizowanych w Krakowskiej Akademii im Andrzeja Frycza Modrzewskiego na Wydziale Nauk o Bezpieczeństwie. Zajęcia z przedmiotu „Podstawy bezpieczeństwa cybernetycznego”, który jest realizowany od 2016 roku, z założenia powinien spełniać większość wymagań stawianych przez wymienione dokumenty i wytyczne.

Zaprezentowana dysertacja, składa się ze wstępu, z rozdziału pierwszego, w którym przedstawiona została polemiczna analiza materiału dotyczącego podstawowych pojęć
w rozpatrywanym obszarze badań. Ponadto przybliżona i scharakteryzowana została cyberprzestrzeń, cyberbezpieczeństwo z perspektywy występujących zagrożeń. W rozdziale drugim, będącym metodologią badań własnych, przedstawiono przedmiot i cele badań, problemy i  hipotezy badawcze, zmienne i wskaźniki oraz metody, techniki i narzędzia badawcze. Omówiono w nim także zaplanowane sposoby weryfikacji wyników badań, scharakteryzowano grupę badawczą i opisano organizację badań. Rozdział trzeci prezentuje szczegółową analizę danych zebranych podczas badań. Składa się z ośmiu podrozdziałów przyporządkowanych do przyjętych problemów szczegółowych. Ósmy, ostatni podrozdział, prezentuje nowatorskie podejście zaproponowane przez autora dysertacji, dotyczące sposobu kształcenia w zakresie bezpieczeństwa w  cyberprzestrzeni. Treści poszczególnych rozdziałów i podrozdziałów zilustrowane zostały rysunkami, wykresami i tabelami. Zakończenie i wnioski zawierają konkluzje o zrealizowaniu celu pracy odnoszące się do całości dysertacji. Ponadto praca zawiera bibliografię, całość dopełnia spis tabel, wykresów, rysunków oraz załączniki.

1. CERT – Computer Emergency Response Team. [↑](#footnote-ref-1)