Technologie informacyjno-komunikacyjne zrewolucjonizowały kluczowe wymiary funkcjonowania współczesnych wspólnot narodowych oraz międzynarodowych. Od wymiany dóbr, poprzez tworzenie oraz utrzymywanie więzi społecznych, aż po zapewnienie kluczowych usług publicznych, technologie te stały się podstawą dla społeczeństw opartych na akumulacji oraz przepływie informacji. Coraz większa zależność od procesów umożliwianych oraz podtrzymywanych za pomocą wspomnianych technologii sprawiła jednak, iż wspólnoty, instytucje, a nawet całe aparaty państwowe stały się podatne na zagrożenia wynikające z charakterystyki funkcjonowania TIK. Z perspektywy technologicznej, ze względu na wysoką homogeniczność systemów komputerowych (zarówno sprzętu, jak i oprogramowania) zestaw kluczowych cyberzagrożeń na całym świecie jest wielce uniwersalny. Niemniej w świetle procesów intersubiektywnego konstruowania zagrożeń w ramach wspólnot narodowych, a także (choć rzadziej) społeczności międzynarodowych, percepcja niebezpieczeństw wynikających z TIK zależy w znacznej mierze od czynników społecznych, kulturowych, ekonomiczno-finansowych, a nawet ideologicznych. Kluczowym zadaniem staje zatem badanie dynamiki konstruowania zagrożeń utożsamianych z problemami cyberbezpieczeństwa w ramach określonych wspólnot. Jako szczególnie ważny poziom tej analizy wskazać należy wspólnoty narodowe, ponieważ to w ich ramach podejmowane są następnie określone działania o charakterze strategicznym, legislacyjnym oraz regulacyjnym w odniesieniu do problematyki cyberbezpieczeństwa.

Problem jednoznacznego określenia zakresu przedmiotowego oraz funkcjonalnego pojęcia cyberbezpieczeństwa stanowi punkt wyjścia do badań na temat odmiennych dyskursów cyberbezpieczeństwa obecnych w polskiej debacie publicznej. Ważną cechą omawianego tematu jest fakt zależności procesów społecznych odpowiedzialnych za wytwarzanie określonych narracji cyberbezpieczeństwa zarówno od warstwy technologicznej określonych problemów i zagrożeń, jak i uwarunkowań politycznych, społecznych oraz ekonomicznych.

W ramach projektu podjęty zostanie szereg działań badawczych, w tym stworzenie ramy teoretycznej dla badania dyskursów cyberbezpieczeństwa, dokonanie analizy oficjalnych źródeł pisanych oraz mówionych, wykorzystanie obserwacji uczestniczącej podczas szeregu konferencji branżowych oraz *public policy* w celu zebrania materiału badawczego, przeprowadzenie ankiet wśród polskich uczestników Europejskiego Forum Cyberbezpieczeństwa CYBERSEC, przeprowadzenie wywiadów półustrukturyzowanych z przedstawicielami administracji publicznej, trzeciego sektora oraz biznesu zaangażowanych w tworzenie dyskursów cyberbezpieczeństwa w Polsce.