Katalog zadań

Planu działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa

Kierunek interwencji	Zadanie	Charakter
Cel szczegółowy 1. Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa		
Kierunek interwencji 1.1. Dostosowanie otoczenia prawnego do potrzeb i wyzwań w obszarze cyberbezpieczeństwa	**zadanie 1.1.1** Opracowanie podstaw prawnych krajowego systemu cyberbezpieczeństwa	P
	zadanie 1.1.2 Umieszczenie w systemie prawnym instytucji i ról krajowego sytemu cyberbezpieczeństwa (w ramach działania 1.1.1)	P
	zadanie 1.1.3 Opracowanie słownika terminologii z obszaru cyberbezpieczeństwa używanej w aktach prawnych	P
	zadanie 1.1.4 Dokonanie przeglądu istniejących regulacji prawnych, sektorowych i szczególnych, które dotyczą lub wymagają uzupełnienia o zakres cyberbezpieczeństwa. (w ramach zadania 1.1.1)	P
	zadanie 1.1.5 Uregulowanie kwestii współpracy operacyjnej, w tym właściwej koordynacji działań i wymiany informacji pomiędzy instytucjami odpowiedzialnymi za bezpieczeństwo narodowe, działania antyterrorystyczne oraz bezpieczeństwo wewnętrzne i porządek publiczny.(w ramach zadania 1.1.1)	P
	zadanie 1.1.6 Okresowe monitorowanie zjawisk zachodzących w obszarze cyberbezpieczeństwa i inicjowanie ewentualnych zmian w przepisach prawa.	C
Kierunek interwencji 1.2 Udoskonalenie	**zadanie 1.2.1** Określenie obowiązków i uprawnień uczestników krajowego systemu cyberbezpieczeństwa . Identyfikacja procesów, ról poszczególnych interesariuszy i ich zasobów w celu skonsolidowania i zharmonizowania działań wszystkich interesariuszy. Doprecyzowanie wzajemnych powiązań pomiędzy poszczególnymi interesariuszami krajowego systemu cyberbezpieczeństwa, w tym organami odpowiedzialnymi za bezpieczeństwo narodowe, działania antyterrorystyczne, bezpieczeństwo wewnętrzne oraz porządek publiczny, prokuraturę oraz sądownictwo. (efekt działania ujęty w ramach zadania 1.1.1)	P
	zadanie 1.2.2 Opracowanie koncepcji zmapowania zasobów osobowych i kompetencyjnych; prowadzenie rejestru/bazy danych tych zasobów cyberbezpieczeństwa (projekt mapowania i wykonanie narzędzi, ciągłe – prowadzenie bazy)	P/C

Kierunek interwencji	Zadanie	Charakter
1.2. Udoskonalenie struktury krajowego systemu cyberbezpieczeństwa	**zadanie 1.2.3** Opracowanie i wdrożenie programu pozyskiwania i retencji ekspertów cyberbezpieczeństwa w administracji państwowej	P/C
	zadanie 1.2.4 Określenie kompetencji organów właściwych, odpowiedzialnych za sprawowanie nadzoru w zakresie systemów teleinformatycznych w sektorach, w których świadczone są usługi kluczowe i usługi cyfrowe.	P
	zadanie 1.2.5 Rozbudowa struktur zajmujących się cyberbezpieczeństwem na poziomie operacyjnym, w tym narodowego centrum cyberbezpieczeństwa (NC Cyber), CSIRT poziomu krajowego, sektorowych zespołów reagowania na incydenty , centrów wymiany i analizy informacji.	P
	zadanie 1.2.6 Utworzenie klastrów bezpieczeństwa dla administracji samorządowej. (komentarz - w ramach RKB)	P
Kierunek interwencji 1.3. Zwiększenie efektywności współdziałania podmiotów zapewniających bezpieczeństwo cyberprzestrzeni RP	**zadanie 1.3.1** Budowa zintegrowanego systemu wymiany informacji	P
	zadanie 1.3.2 Przygotowanie programu ćwiczeń i treningów w skali kraju i w skali poszczególnych sektorów	P
	zadanie 1.3.3 Aktywny udział w ćwiczeniach prowadzonych zarówno przez organizacje krajowe, podmioty UE i NATO oraz inne podmioty międzynarodowe.	C
	zadanie 1.3.4 Przystąpienie do zaufanych międzynarodowych forów wymiany informacji o zagrożeniach w cyberprzestrzeni.	P
Kierunek interwencji 1.4. Zwiększenie bezpieczeństwa teleinformatycznego usług kluczowych i	**zadanie 1.4.1** Opracowywanie standardowych procedur operacyjnych dotyczących współpracy w obsłudze incydentu w cyberprzestrzeni, w tym schematów raportowania dla operatorów usług kluczowych i dostawców usług cyfrowych (zadanie powiązane z 1.3.1)	P
	zadanie 1.4.2 Opracowanie systemu wspierającego analizę współzależności pomiędzy sektorami operatorów usług kluczowych oraz pomiędzy operatorami a dostawcami usług cyfrowych oraz przeprowadzanie analiz na podstawie pozyskanych danych źródłowych	P
	zadanie 1.4.3 Opracowanie kryteriów identyfikacji UK i IK z uwzględnieniem potrzeby ich integracji	P

Kierunek interwencji	Zadanie	Charakter
cyfrowych oraz infrastruktury krytycznej	**zadanie 1.4.4** Opracowanie minimalnych wymagań zapewnienia bezpieczeństwa teleinformatycznego (organizacyjne i techniczne) dla operatorów usług kluczowych (w obszarach IT, OT, kompetencji personelu)	P
	zadanie 1.4.5 Opracowanie metodyki przeprowadzania wewnętrznych i zewnętrznych audytów bezpieczeństwa teleinformatycznego.	P
	zadanie 1.4.6 Opracowanie programu szkolenia dla operatorów IK/UK z zakresu bezpieczeństwa teleinformatycznego (uświadamiające oraz podnoszące kwalifikacje).	P
	zadanie 1.4.7 Budowa Rządowego Klastra Bezpieczeństwa.	P
Kierunek interwencji 1.5. Opracowanie i wdrożenie standardów oraz dobrych praktyk bezpieczeństwa sieci i systemów informatycznych	**zadanie 1.5.1** Opracowanie podręcznika konfiguracji oprogramowania standardowego w typowych zastosowaniach.	P
	zadanie 1.5.2 Przegląd istniejących norm/standardów/dobrych praktyk, ich tłumaczenie i udostępnienie.	P/C
Kierunek interwencji 1.6. Wypracowanie i wdrożenie systemu zarządzania ryzykiem na poziomie krajowym	**zadanie 1.6.1** Stworzenie systemu monitorującego zagrożenia i podatności w trybie rzeczywistym i dokonującego bieżącej oceny ryzyka naruszenia bezpieczeństwa państwa.	P
	zadanie 1.6.2 Wdrożenie systemu zarządzania ciągłością działania w administracji rządowej	P
	zadanie 1.6.3 Opracowanie metodyki szacowania ryzyka naruszenia bezpieczeństwa państwa, uwzględniającej specyfikę poszczególnych sektorów, a także operatorów infrastruktury krytycznej, usług kluczowych i dostawców usług cyfrowych i spójnej z metodyką szacowania ryzyka na potrzeby raportu o stanie bezpieczeństwa państwa.	P

Kierunek interwencji	Zadanie	Charakter
Kierunek interwencji 1.7. Zapewnienie bezpiecznego łańcucha dostaw	**zadanie 1.7.1** Zbudowanie krajowego systemu oceny i certyfikacji wyrobów sektora IT i uzyskanie pełnego członkostwa w SOGIS MRA	P
	zadanie 1.7.2 Opracowanie modelu bezpiecznego łańcucha dostaw (zadanie powiązane z 1.7.1)	P
Kierunek interwencji 1.8. Zbudowanie systemu ostrzegania użytkowników cyberprzestrzeni w zakresie ryzyka wynikającego z cyberzagrożeń	**zadanie 1.8.1** Zbudowanie systemu bieżącego zarządzania bezpieczeństwem cyberprzestrzeni, który na podstawie zgłaszanych informacji o zagrożeniach i podatnościach, umożliwi ich agregowane, analizowanie i korelowanie, a także wypracowanie ostrzeżeń na temat zagrożeń i podatności i przekazywanie ich do zainteresowanych stron w taki sposób, aby zachowane zostały zasady poufności informacji przekazywanych w zgłoszeniach.	P
	zadanie 1.8.2 Utworzenie systemu informacyjnego dla obywateli, w celu ochrony użytkowników końcowych przed skutkami zidentyfikowanych zagrożeń.	P
Cel szczegółowy 2. Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom		
Kierunek interwencji 2.1. Zwiększanie zdolności do zwalczania	**zadanie 2.1.**1 współpraca z operatorami usług kluczowych, dostawcami usług cyfrowych oraz operatorami infrastruktury krytycznej w wykrywaniu oraz zwalczaniu incydentów o charakterze cyberprzestępczości, w tym cyberszpiegostwa, zdarzeń o charakterze terrorystycznym oraz działań o charakterze hybrydowym we wszystkich ich fazach.	C
	zadanie 2.1.2 Monitorowanie efektywności czynności operacyjnych i procesowych w obszarze zwalczania cyberprzestępczości.	C
	zadanie 2.1.3 Transgraniczna współpraca organów ścigania oraz podmiotów typu CERT/CSIRT	C
	zadanie 2.1.4 Ujednolicenie słownika pojęć stosowanych przez organy ścigania i wymiar sprawiedliwości w obszarze walki z cyberprzestępczością.	P
	zadanie 2.1.5 Ustandaryzowanie statystyk opracowywanych przez organy ścigania w obszarze walki z cyberprzestępczością.	P

Kierunek interwencji	Zadanie	Charakter
zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym, występującej w cyberprzestrzeni	**zadanie 2.1.6** Stworzenie rozwiązań prawnych i procedur pozwalających na współpracę organów ścigania z podmiotami prywatnymi w zakresie walki z cyberprzestępczością (zadanie powiązane z 1.1.1)	P
	zadanie 2.1.7 Budowa sieci/forum współpracy organów ścigania i sędziów zajmujących się problematyką cyberprzestępczości (zadanie powiązane z 1.1.1).	P
	zadanie 2.1.8 Organizacja systemu obowiązkowych szkoleń dla przedstawicieli organów ścigania i wymiaru sprawiedliwości zajmujących się zwalczaniem cyberprzestępczości (zadanie powiązane z 1.1.1).	P
	zadanie 2.1.10 Przegląd i dostosowanie kodeksu karnego, kodeksu postępowania karnego do aktualnych potrzeb zwalczania cyberprzestępczości, cyberterroryzmu itp.	P
Kierunek interwencji 2.2. Uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni	**zadanie 2.2.1** Uregulowanie obszaru wytwarzania, posiadania, pozyskiwania oraz wykorzystywania specjalistycznych narzędzi z zakresu prowadzenia działań militarnych w cyberprzestrzeni przez resort obrony narodowej.	P
	zadanie 2.2.2 Podnoszenie zdolności Sił Zbrojnych Rzeczypospolitej Polskiej (SZ RP) do prowadzenia działań militarnych w cyberprzestrzeni w ramach ćwiczeń krajowych i międzynarodowych.	C
	zadanie 2.2.3 Uwzględnienie w działaniach militarnych w cyberprzestrzeni: rozpoznawania zagrożeń, ochrony i obrony systemów teleinformatycznych oraz zwalczania źródeł zagrożeń.	C
	zadanie 2.2.4 Włączenie działań w cyberprzestrzeni w planowanie operacyjne, jako integralna część operacji prowadzonych przez SZ RP samodzielnie, jak i w układzie sojuszniczym oraz koalicyjnym.	C
	zadanie 2.2.5 Udoskonalenie struktur wojskowych, które zapewnią skuteczniejsze planowanie, dowodzenie i zarządzanie zasobami, umiejętnościami i zdolnościami.	C
	zadanie 2.2.6 Stałe podnoszenie umiejętności personelu prowadzącego działania militarne w cyberprzestrzeni w ramach szkoleń wewnętrznych, jak i wysoce specjalistycznych szkoleń zewnętrznych przygotowywanych na potrzeby resortu obrony narodowej.	C

Kierunek interwencji	Zadanie	Charakter
	zadanie 2.2.7 Prowadzenie bieżącego rozpoznania zagrożeń oraz oceny sytuacji w celu podjęcia właściwych środków ochrony lub aktywnego przeciwdziałania źródłom zagrożeń.	C
	zadanie 2.2.8 Wytwarzanie bądź pozyskiwanie nowatorskich narzędzi służących do podniesienia skuteczności działań militarnych w cyberprzestrzeni.	P
Kierunek interwencji 2.3. Zbudowanie zdolności w zakresie analizy zagrożeń na poziomie krajowym	**zadanie 2.3.1** Rozbudowanie zdolności analitycznych CERT Polska i NC Cyber w taki sposób aby uzyskać pełne spektrum zdolności analitycznych w cyberprzestrzeni na poziomie krajowym (powiązane z zadaniem 1.8.1)	P
	zadanie 2.3.2 Stworzenie narzędzi badawczych pozwalających na prowadzenie zaawansowanych analiz na big data w obszarze cyberbezpieczeństwa	P
	zadanie 2.3.3 Wypracowanie zdolności kształcenia i rozwoju wykwalifikowanego personelu dla prowadzenia zadań analitycznych	P
	zadanie 2.3.4 Rozwijanie możliwości prowadzenia projektów badawczych w oparciu o dane pozyskane w ramach funkcjonowania krajowego systemu cyberbezpieczeństwa	C
Kierunek interwencji 2.4. Zbudowanie systemu bezpiecznej komunikacji na potrzeby bezpieczeństwa narodowego	**zadanie 2.4.1** Zbudowanie spójnego systemu łączności jawnej i niejawnej całej administracji rządowej na potrzeby systemu kierowania bezpieczeństwem narodowym.	P

Kierunek interwencji	Zadanie	Charakter
Kierunek interwencji 2.5. Audyty i testy bezpieczeństwa	**zadanie 2.5.1** Opracowanie spójnej metodyki audytów, na podstawie norm i dobrych praktyk oraz uwzględniając specyfiki poszczególnych sektorów	P
	zadanie 2.5.2 Opracowanie metodyki testów penetracyjnych.	P
	zadanie 2.5.3 Utworzenie repozytorium audytów i testów	P
	zadanie 2.5.4 Uregulowanie przygotowania i posiadania specjalistycznych narzędzi do prowadzenia testów penetracyjnych oraz ich prowadzenie.	P
Cel szczegółowy 3. **Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni**		
Kierunek interwencji 3.1. Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa	**zadanie 3.1.1** Uruchomienie programu Cyberpark Enigma.	P
	zadanie 3.1.2 Uruchomienie hubów innowacyjności.	P
	zadanie 3.1.3 Budowa sieci laboratoriów na uczelniach / Powstanie Naukowego Klastra Cyberbezpieczeństwa (NKC)	P
	zadanie 3.1.4 Inwestowanie w rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa poprzez stwarzanie warunków dla rozwoju przedsiębiorstw, ośrodków naukowo-badawczych, jak i start-up'ów, których przedmiotem działalności jest tworzenie nowych rozwiązań, tym w obszarze cyberbezpieczeństwa.	C
Kierunek interwencji 3.2. Zbudowanie mechanizmów współpracy między sektorem publicznym i prywatnym	**zadanie 3.2.1** Rozbudowana systemów partnerskich w NC Cyber	P
	zadanie 3.2.2 Budowa systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa.	P
	zadanie 3.3.1 Uruchomienie w NCBiR programów badawczo-rozwojowych w obszarze cyberbezpieczeństwa / Przygotowanie projektów w ramach HORYZONT 2020	P

Kierunek interwencji	Zadanie	Charakter
Kierunek interwencji 3.3. Stymulowanie badań i rozwoju w obszarze bezpieczeństwa systemów teleinformatycznych	**zadanie 3.3.2** Doradztwo w zakresie określania kierunków badań	C
	zadanie 3.3.3 Opracowanie programów badawczych we współpracy ze środowiskiem naukowo-badawczym.	P
	zadanie 3.3.4 Opracowanie zadań w systemie zapewnienia cyberbezpieczeństwa dla organizacji pozarządowych.	P
	zadanie 3.3.5 Uruchomienie naboru/programu pozyskania specjalistów o unikatowych umiejętnościach przez ośrodki analityczne na potrzeby rozwiązywania skomplikowanych problemów z zakresu cyberbezpieczeństwa	P
Kierunek interwencji 3.4. Zwiększanie kompetencji kadry podmiotów istotnych dla funkcjonowania bezpieczeństwa	**zadanie 3.4.1** Rozwój działań prowadzonych w ramach Akademii NASK	C
	zadanie 3.4.2 Opracowanie i wdrożenie systemu obligatoryjnych, cyklicznych szkoleń i ćwiczeń kadr administracji państwowej na wszystkich szczeblach, dostosowanych do wykonywanych zadań (zadanie powiązane z 1.1.1)	P
	zadanie 3.4.3 Ustanowienie programu stypendialnego „Złota Setka” (powiązane z zadaniem 3.3.5)	P
	zadanie 3.4.4 Opracowanie programów studiów dla szkół wyższych w specjalnościach z zakresu cyberbezpieczeństwa	P
	zadanie 3.4.5 Ustanowienie nowych zawodów i specjalności w obszarze cyberbezpieczeństwa	P

Kierunek interwencji	Zadanie	Charakter
bezpieczeństwa cyberprzestrzeni	**zadanie 3.4.6** Zachęcanie uczelni do rozwijania specjalizacji interdyscyplinarnych obejmujących między innymi zarządzanie bezpieczeństwem informacji, ochronę danych osobowych, ochronę własności intelektualnej w Internecie oraz zagadnienia związane z rozwojem nowych technologii i wyzwaniami, które są tego pochodnymi.	C
	zadanie 3.4.8 Opracowanie modelu zarządzania zasobami ludzkimi w obszarze cyberbezpieczeństwa.	P
Kierunek interwencji 3.5. Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli	**zadanie 3.5.1** Uwzględnienie tematyki bezpieczeństwa informacyjnego w programach nauczania szkół podstawowych i średnich. / Opracowanie wkładów do programu nauczania	P
	zadanie 3.5.2 Opracowanie i realizacja planu doskonalenia zawodowego nauczycieli odpowiedzialnych za nauczanie w zakresie bezpieczeństwa informacyjnego w szkołach.	P/C
	zadanie 3.5.3 Opracowanie i realizacja planu podnoszenia świadomości społecznej w obszarze cyberbezpieczeństwa; prewencja cyberprzestępczości; koordynacja inicjatyw/kampanii społecznych podejmowanych przez poszczególne instytucje, organizacje pozarządowe, sektor prywatny.	P
Cel szczegółowy 4. Zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa		
	zadanie 4.1.1 Udział w pracach i dyskusjach prowadzonych na forum UE, w tym Horyzontalnej Grupy Roboczej Rady UE ds. Cyberbezpieczeństwa.	C
	zadanie 4.1.2 Udział w pracach i dyskusjach prowadzonych na forum NATO, w tym Komitetu Obrony Cybernetycznej	C
	zadanie 4.1.3 Przeprowadzenie kampanii na rzecz uzyskania miejsca w kolejnej Grupie Ekspertów Rządowych ds. cyberbezpieczeństwa (w przypadku decyzji ZO ONZ o powołaniu w grupy w kolejnych latach).	P
	zadanie 4.1.4 Udział w pracach i dyskusjach prowadzonych na forum OBWE, szczególnie Nieformalnej Grupy Roboczej ds. Środków Budowy Zaufania.	C

Kierunek interwencji	Zadanie	Charakter
Kierunek interwencji 4.1. Aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym	**zadanie 4.1.5** Udział w pracach i dyskusjach prowadzonych na forum innych organizacji, w tym m.in. Rady Europy (Komitet Konwencji ws. Cyberprzestępczości) i OECD.	C
	zadanie 4.1.6 Udział w pracach i dyskusjach prowadzonych na forach regionalnych, takich jak m.in. Grupa Wyszehradzka (Platforma Cyberbezpieczeństwa Państw Europy Centralnej).	C
	zadanie 4.1.7 Włączanie problematyki bezpieczeństwa cybernetycznego do agendy konsultacji z zakresu polityki bezpieczeństwa i współpracy dwustronnej oraz organizacja odrębnych dwustronnych konsultacji z zakresu bezpieczeństwa cybernetycznego z wybranymi sojusznikami i partnerami.	C
	zadanie 4.1.8 Prowadzenie przez Ministerstwo Cyfryzacji oraz NASK/NC Cyber współpracy z ENISĄ na poziomie strategiczno-politycznym	C
	zadanie 4.1.9 Budowanie w NC Cyber zdolności w zakresie wsparcia analitycznego dla administracji publicznej w obszarze strategicznym (policy).	P
	zadanie 4.1.10 Wypracowanie krajowego stanowiska/celów dot. polityki cyberbezpieczeństwa, jakie będzie prezentowane na arenie międzynarodowej przez wszystkie instytucje (nie dotyczy obsługiwanych przez poszczególne resorty grup roboczych w RUE).	P
	zadanie 4.1.11 Utworzenie funkcji „ambasadora ds. bezpieczeństwa cyberprzestrzeni", odpowiedzialnego za reprezentowanie RP w zakresie cyberbezpieczeństwa/innowacji/nowych technologii w kontaktach z innymi państwami, instytucjami międzynarodowymi, sektorem prywatnym; odpowiedzialnego za koordynację uzgodnień krajowego stanowiska w obszarach cyberbezpieczeństwa/ innowacji/nowych technologii na arenie międzynarodowej ale też kontakty z biznesem i przyciąganie nowych inwestycji z zakresu cyberbezpieczeństwa do Polski (commercial diplomacy).	P
	zadanie 4.1.12 Opracowanie planu i prowadzenie nadzoru nad kampaniami promującymi Polskę i polskich przedsiębiorców.	P/C
	zadanie 4.1.13 Promowanie na arenie międzynarodowej organizowanych na terenie Polski konferencji poświęconych tematyce cyberbezpieczeństwa.	C
	zadanie 4.1.14 Włączanie problematyki cyberbezpieczeństwa do agendy konsultacji w ramach współpracy dwustronnej oraz organizacja odrębnych dwustronnych konsultacji z zakresu cyberbezpieczeństwa z wybranymi sojusznikami i partnerami.	P

Kierunek interwencji	Zadanie	Charakter
Kierunek interwencji 4.2. Aktywna współpraca międzynarodowa na poziomie operacyjnym i technicznym	**zadanie 4.2.1** Opracowanie i promowanie polskiego modelu współpracy w ramach sieci wymiany informacji.	P
	zadanie 4.2.2 Budowa sieci wymiany informacji o zagrożeniach i współpraca na poziomie technicznym/ operacyjnym z siecią CERT/CSIRT P.Cz. UE	P
	zadanie 4.2.3 Wymiana informacji o zagrożeniach i współpraca na poziomie technicznym/operacyjnym z CERT NATO	C
	zadanie 4.2.5 Koordynacja ćwiczeń Cyber Europe	C
	zadanie 4.2.6 Udział CERT Polska w międzynarodowych ćwiczeniach z zakresu cyberbezpieczeństwa	C
	zadanie 4.2.7 Współpraca z ENISĄ na poziomie operacyjnym i technicznym	C
	zadanie 4.2.8 Współpraca CERT Polska z innymi zespołami CERT, udział w projektach i konferencjach	C
	zadanie 4.2.9 Udział CERT Polska w sieci CSIRT powołanej na mocy dyrektywy NIS	C
	zadanie 4.2.11 Udział personelu technicznego w ćwiczeniach z zakresu cyberbezpieczeństwa organizowanych przez NATO	C

P – zadanie o charakterze projektowym C – zadanie o charakterze ciągłym