Projekt z dnia 19.04.2017 r.

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia …….. 2017 r.

w sprawie nadania Naukowej i Akademickiej Sieci Komputerowej statusu państwowego instytutu badawczego

Na podstawie art. 21 ust. 5 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2016 r. poz. 371, 1079, 1311 i 2260 oraz z 2017 r. poz. 202) zarządza się, co następuje:

§ 1. 1. Naukowej i Akademickiej Sieci Komputerowej w Warszawie, zwanej dalej „NASK”, utworzonej na podstawie zarządzenia nr 5/93 Przewodniczącego Komitetu Badań Naukowych z dnia 14 grudnia 1993 r. w sprawie utworzenia jednostki badawczo-rozwojowej pod nazwą Naukowa i Akademicka Sieć Komputerowa (Dz. Urz. KBN Nr 7 poz. 33), nadaje się status państwowego instytutu badawczego.

2. Instytut używa nazwy „Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy”.

3. Nadzór nad NASK sprawuje minister właściwy do spraw informatyzacji.

§ 2. Przedmiotem działania NASK jest:

1) prowadzenie badań naukowych i prac rozwojowych w zakresie:
   a) telekomunikacji,
   b) teleinformatyki,
   c) informatyki,
   d) cyberbezpieczeństwa,
   e) funkcjonowania polskiego rejestru domen internetowych,
   f) społeczeństwa informacyjnego;
2) przystosowywania wyników badań naukowych i prac rozwojowych do potrzeb praktyki;
3) wdrażania wyników badań naukowych i prac rozwojowych w usługach świadczonych między innymi na potrzeby organów bezpieczeństwa i porządku publicznego, bezpieczeństwa państwa oraz bezpieczeństwa jednostek infrastruktury krytycznej.

§ 3. 1. Do podstawowych zadań NASK należy:

1) prowadzenie badań naukowych i prac rozwojowych finansowanych ze środków finansowych na naukę, którymi dysponuje minister właściwy do spraw nauki;
2) prowadzenie badań naukowych i prac rozwojowych finansowanych z innych źródeł, w tym także ze środków Unii Europejskiej i środków Paktu Północnoatlantyckiego;
3) opracowywanie opinii i ekspertyz w zakresie prowadzonych badań naukowych i prac rozwojowych;
4) wytwarzanie w związku z prowadzonymi badaniami naukowymi i pracami rozwojowymi oprogramowania, aparatury, urządzeń i innych wyrobów;
5) prowadzenie badań naukowych i wdrożeniowych w zakresie ochrony informacji i systemów informacyjnych;
6) prowadzenie badań naukowych i wdrożeniowych w zakresie ochrony infrastruktury telekomunikacyjnej i teleinformatycznej administracji publicznej;
7) realizowanie zadań nałożonych na NASK przez ministra nadzorującego – jeżeli jest to niezbędne ze względu na potrzeby obronności i bezpieczeństwa publicznego, w przypadku klęski żywiołowej lub w celu wykonania zobowiązań międzynarodowych;
8) prowadzenie działalności wydawniczej związanej z prowadzonymi badaniami naukowymi i pracami rozwojowymi;
9) organizowanie kursów i konferencji naukowych krajowych i międzynarodowych związanych z prowadzonymi badaniami naukowymi i pracami rozwojowymi;
10) prowadzenie innych form kształcenia, w tym szkoleń i kursów dokształcających;
11) opracowywanie i wdrażanie usług telekomunikacyjnych, teleinformatycznych, informatycznych oraz z zakresu bezpieczeństwa sieci i systemów teleinformatycznych oraz dziedzin pokrewnych;
12) wykonywanie innych zadań zleconych przez ministra właściwego do spraw informatyzacji.

2. Do zadań NASK, szczególnie ważnych dla planowania i realizacji polityki państwa, których wykonywanie jest niezbędne do zapewnienia bezpieczeństwa publicznego, rozwoju edukacji oraz poprawy jakości życia obywateli, wykonywanych w sposób ciągły należy:

1) zapewnienie cyberbezpieczeństwa podmiotom publicznym w zakresie zlecanym i wskazywanym przez ministra właściwego do spraw informatyzacji lub inne organy administracji publicznej, poprzez:

a) realizację projektów związanych z bezpieczeństwem cyberprzestrzeni Rzeczypospolitej Polskiej,
b) tworzenie narzędzi do monitorowania sieci bot-net,
c) utrzymanie operacyjnego centrum zarządzania cyberbezpieczeństwem sfery cywilnej,
d) rozwój Narodowego Centrum Cyberbezpieczeństwa (NC Cyber);

2) wsparcie w budowie Polski Cyfrowej polegające w szczególności na rozwoju bezpiecznej infrastruktury teleinformatycznej dla nauki (WARMAN) i realizacji projektu Ogólnopolskiej Sieci Edukacyjnej (OSE);

3) prowadzenie badań naukowych i prac rozwojowych ukierunkowanych na ich wdrożenie wspomagających:
a) rozwój systemów identyfikacji, w tym biometrii,
b) uczenie maszynowe i sztuczną inteligencję,
c) modelowanie, symulację i optymalizację w systemach sieciowych,
d) cyberbezpieczeństwo,
e) przetwarzanie dużych, zmiennych i różnorodnych danych, w tym w chmurach obliczeniowych,
f) metody analiz sieci społecznych,
g) rozwój „Internetu Rzeczy" (*IoT*),
h) technologię „blockchain";

4) rozwój społeczeństwa informacyjnego i badania nad bezpieczeństwem korzystania z sieci, szczególnie przez dzieci.

§ 4. Źródłem finansowania zadań NASK są środki finansowe:

1) uzyskane z przychodów własnych w związku z prowadzoną działalnością, w szczególności badawczo-rozwojową oraz gospodarczą;
2) pochodzące z dotacji lub dotacji celowych uzyskiwanych na zasadach określonych w ustawie z dnia 30 kwietnia 2010 r. o instytutach badawczych oraz w innych przepisach;
3) pozyskiwane przez NASK na realizację projektów finansowanych z funduszy Unii Europejskiej lub innych funduszy zagranicznych;
4) uzyskiwane z innych źródeł.

§ 5. Dysponentem środków budżetowych ustalanych na realizację zadań, o których mowa w § 3 ust. 2, jest minister właściwy do spraw informatyzacji.

§ 6. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

MINISTER CYFRYZACJI

Za zgodność pod względem prawnym,
legislacyjnym i redakcyjnym
Aleksandra Ostapiuk
Dyrektor Departamentu Prawnego
w Ministerstwie Cyfryzacji
/-podpisano elektronicznie/

UZASADNIENIE

Przedmiotowe rozporządzenie ma na celu zmianę statusu Naukowej i Akademickiej Sieci Komputerowej z instytutu badawczego na państwowy instytut badawczy.

Naukowa i Akademicka Sieć Komputerowa– Instytut Badawczy (NASK) została utworzona na podstawie zarządzenia nr 5/93 Przewodniczącego Komitetu Badań Naukowych z dnia 14 grudnia 1993 r. w sprawie utworzenia jednostki badawczo-rozwojowej pod nazwą Naukowa i Akademicka Sieć Komputerowa (Dz. Urz. KBN Nr 7 poz. 33).

NASK, jako instytut badawczy działa obecnie na podstawie statutu uchwalonego przez Radę Naukową NASK w dniu 16 lutego 2011 r. (zatwierdzonego Zarządzeniem28/2011 z dnia 25 marca 2011 r. Ministra Nauki i Szkolnictwa Wyższego (Dz. Urz. z 2011, poz. 32), zmienionego Uchwałą Rady Naukowej NASK w dniu 6 czerwca 2014 r., zatwierdzonego Zarządzeniem z dnia 11 lipca 2014 r. Ministra Nauki i Szkolnictwa Wyższego, Dz. Urz. MNiSW poz. 40) oraz zmienionego Decyzją Ministra Cyfryzacji nr 25 z dnia 30 sierpnia 2016 r. (Dz.Urz. MC poz. 36).

Wydanie rozporządzenia Rady Ministrów w sprawie nadania Naukowej i Akademickiej Sieci Komputerowej statusu państwowego instytutu badawczego, dokonywane jest na podstawie art. 21 ust. 5 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2016 r. poz. 371, 1079, 1311 i 2260 oraz z 2017 r. poz. 202).

Nadanie statusu państwowego instytut badawczego Naukowej i Akademickiej Sieci Komputerowej ma umożliwić powierzenie instytutowi na podstawie art. 22 pkt 2 lit. a ustawy o instytutach badawczych zadań ciągłych szczególnie ważnych dla planowania i realizacji polityki państwa, których wykonywanie jest niezbędne do zapewnienia bezpieczeństwa publicznego, rozwoju edukacji oraz poprawy jakości życia obywateli, wykonywanych w sposób ciągły, a w szczególności:

1) zapewnienie cyberbezpieczeństwa podmiotom publicznym w zakresie zlecanym i wskazywanym przez ministra właściwego do spraw informatyzacji lub inne organy administracji publicznej, poprzez:
   a) realizację projektów związanych z bezpieczeństwem cyberprzestrzeni Rzeczypospolitej Polskiej,
   b) tworzenie narzędzi do monitorowania sieci bot-net,

c) utrzymanie operacyjnego centrum zarządzania cyberbezpieczeństwem sfery cywilnej,

d) rozwój Narodowego Centrum Cyberbezpieczeństwa (NC Cyber);

2) wsparcie w budowie Polski Cyfrowej polegające w szczególności na rozwoju bezpiecznej infrastruktury teleinformatycznej dla nauki (WARMAN) i realizacji projektu Ogólnopolskiej Sieci Edukacyjnej (OSE);

3) prowadzenie badań naukowych i prac rozwojowych ukierunkowanych na ich wdrożenie wspomagających:

a) rozwój systemów identyfikacji, w tym biometrii,

b) uczenie maszynowe i sztuczną inteligencję,

c) modelowanie, symulację i optymalizację w systemach sieciowych,

d) cyberbezpieczeństwo,

e) przetwarzanie dużych, zmiennych i różnorodnych danych, w tym w chmurach obliczeniowych,

f) metody analiz sieci społecznych,

g) rozwój „Internetu Rzeczy" (*IoT*),

h) technologię „blockchain";

4) rozwój społeczeństwa informacyjnego i badania nad bezpieczeństwem korzystania z sieci, szczególnie przez dzieci.

Celami projektów związanych z bezpieczeństwem cyberprzestrzeni Rzeczypospolitej Polskiej są: zbudowanie bezpiecznej architektury systemów teleinformatycznych Państwa (składającej się z centrum przetwarzania danych i rozległej sieci komputerowej umożliwiającej bezpieczne łączenie się podmiotów rządowych pomiędzy sobą, z siecią Internet oraz świadczenie usług dla obywateli jak ePUAP, źródło, obywatel.gov.pl.), objęcie monitorowaniem i korelacją zdarzeń kluczowych usług informatycznych zapewniających bezpieczeństwo funkcjonowania Państwa, obywateli i podmiotów gospodarczych, dostarczenie rozwiązań, które umożliwią dostęp do bieżącej informacji o stanie bezpieczeństwa teleinformatycznego niezbędnego do oceny sytuacji i stanu bezpieczeństwa w cyberprzestrzeni w Polsce oraz koordynacji reagowania na incydenty komputerowe na poziomie krajowym. Efektami projektów będą: podniesienie poziomu bezpieczeństwa funkcjonowania podmiotów państwowych poprzez zwiększenie odporności na ataki DDoS, możliwość wykrywania ataków na punktach styków, zwiększenie poufności informacji poprzez implementacje usług zarządzania informacją, podniesienie poziomu bezpieczeństwa funkcjonowania podmiotów

państwowych, firm i obywateli w cyberprzestrzeni. Efekty mają być zrealizowane poprzez objęcie monitorowaniem systemów teleinformatycznych wykorzystywanych w procesach kierowania Państwem, a w szczególności służących komunikowaniu się pomiędzy organami władzy publicznej oraz władzą publiczną i społeczeństwem. Ponadto, także przeznaczonych do świadczenia usług kluczowych, które muszą posiadać odporność na zakłócenia wywołane zarówno przez czynniki zewnętrzne, jak i wewnętrzne.

Projekt „tworzenie narzędzi do monitorowania sieci bot-net" polega na analizie działań sieci bot-net oraz stworzeniu narzędzi pozwalających na skuteczne monitorowanie sieci bot-net celem analizy zagrożenia, które mogą spowodować, jej mitygacji a także wykrywaniu nowych, powstających bot-netów oraz monitorowaniu ich działania.

Zadanie „utrzymanie operacyjnego centrum zarządzania cyberbezpieczeństwem sfery cywilnej" związane jest z utrzymaniem centrum w trybie pracy ciągłej 24/7/365. Zadanie związane jest z zarządzeniem incydentami, które będą zgłaszane do Narodowego Centrum Cyberbezpieczeństwa (znajdującego się w strukturze NASK). Ponadto, zadanie polega na zwiększeniu możliwości reagowania na zmaterializowane zagrożenia w cyberprzestrzeni Rzeczypospolitej Polskiej, tj. utrzymanie zdolności do całodobowej gotowości w zakresie reagowania na incydenty komputerowe, wsparcie jednostek sektorowych, możliwość wykrywania zagrożeń ponadsektorowych. Centrum będzie traktowane jako całodobowy punkt wymiany informacji oraz będzie dostarczać bieżącej informacji o bezpieczeństwie cyberprzestrzeni oraz w poszczególnych sektorach. Mechanizmy zaimplementowane w Centrum pozwolą na alarmowanie w przypadku wystąpienia poważnych cyberataków w cyberprzestrzeni Rzeczypospolitej Polskiej.

Instytut po zmianie statusu będzie wspierał budowę Polski Cyfrowej w szczególności w obszarze rozwoju bezpiecznej infrastruktury teleinformatycznej dla nauki i edukacji.Naukowa i Akademicka Sieć Komputerowa (NASK) już od 2016 roku, na zlecenie Ministra Cyfryzacji, rozpoczęła pilotażowy program, doprowadzenia do szkół łączy o przepustowości 1 Gb/s. Celem tego programu jest:

1) opracowanie i wdrożenie technicznego modelu dostępu do bezpiecznego szerokopasmowego internetu w szkołach podstawowych, gimnazjalnych i ponadgimnazjalnych;
2) uzyskanie danych kosztowych oraz ruchowych do prawidłowego opracowania projektu budowy ogólnopolskiej sieci łączącej szkoły podstawowe i ponadpodstawowe;

3) udostępnienie multimedialnych aplikacji i serwisów o charakterze dydaktycznym.

Wspólna inicjatywa Ministerstwa Cyfryzacji, Ministerstwa Nauki i Szkolnictwa Wyższego oraz Ministerstwa Edukacji Narodowej zakłada podłączenie do szybkich łączy wszystkich jednostek oświatowych w Polsce. Zamierzenie to funkcjonujące pod nazwą Ogólnopolska Sieć Edukacyjna (OSE) jest jednym z kluczowych działań w obszarze rozwoju edukacji i społeczeństwa informacyjnego.

Program ten do chwili obecnej przyniósł wymierne korzyści jednostkom oświaty, które wzięły udział w jego realizacji. Zaowocował też dużą ilością danych dotyczących struktury ruchu generowanego przez jednostki oświaty i jego natężenia, preferencji użytkowników dotyczących wyboru usług edukacyjnych oraz aspektów technicznych funkcjonowania sieci w warunkach szkolnych. W ramach programu, rozwijane są usługi edukacyjne dostępne w tej sieci i tworzone nowe, często rewolucyjne narzędzia edukacyjne.

Projekt OSE został wskazany, jako kluczowy w obszarze Cyfryzacji w Strategii Odpowiedzialnego Rozwoju i zakłada stworzenie sieci dostępu do internetu łączącej wszystkie szkoły w Polsce (ok. 30,5 tys.), co umożliwi wdrożenie innowacyjnych metod nauczania i rozwój edukacji cyfrowej.

Projekt ten wymaga wypracowania przygotowania i późniejszego wdrożenia standardów dla realizacji tej sieci w szczególności w obszarze bezpieczeństwa infrastruktury. Niezbędne jest więc wsparcie ze strony profesjonalnej jednostki posiadającej odpowiednie kompetencje i potencjał do przeprowadzenia tego typu działań.

Ponadto, ważnym zadaniem NASK jest wspieranie rozwoju społeczeństwa informacyjnego i badań nad bezpieczeństwem korzystania z sieci, szczególnie przez dzieci. W tym celu NASK będzie realizował zadania związane z działalnością informacyjną, profilaktyczną i edukacyjną, wspierając przy tym Ministra Cyfryzacji oraz Ministra Edukacji Narodowej.

Ze względu na zakres dotychczasowej działalności, doświadczenie jak również możliwości organizacyjne i techniczne NASK jest najbardziej odpowiednim podmiotem do realizacji ww. działań. Jednak wykonywanie takich zadań przez NASK w sposób ciągły oraz zapewnienie ich finasowania wymaga zmiany statusu tej jednostki na państwowy instytut badawczy. Umożliwi to powierzenie Instytutowi na podstawie art. 22 pkt 2 lit.

a ustawy o instytutach badawczych zadań ciągłych szczególnie ważnego dla planowania i realizacji polityki państwa wskazanych w rozporządzaniu.

Pozwoli to też na wzmocnienie potencjału badawczego i rozwojowego NASK, co przełoży się na sprawniejszą realizację wykonywanych przez tą jednostkę zadań i prac badawczych.

NASK, co do zasady, prowadzi badania naukowe i prace rozwojowe ukierunkowane na ich wdrożenie, które mają wspomagać:

a) rozwój systemów identyfikacji, w tym biometrii,
b) uczenie maszynowe i sztuczną inteligencję,
c) modelowanie, symulację i optymalizację w systemach sieciowych,
d) cyberbezpieczeństwo,
e) przetwarzanie dużych, zmiennych i różnorodnych danych, w tym w chmurach obliczeniowych,
f) metody analiz sieci społecznych,
g) rozwój „Internetu Rzeczy” (IoT),
h) technologię „blockchain”;

Powyższe badania wpływać będą na zwiększenie bezpieczeństwa sieci i systemów informatycznych, w szczególności w obszarach, gdzie przetwarzane są dane osobowe, dane wrażliwe czy też informacje niejawne. Ponadto, prace nad technologią blockchain pozwolą zmniejszyć ryzyko dokonywanych transakcji i uchronić inwestorów przed wszelkiego rodzaju oszustwom i malwersacjom.

Projektowane rozporządzenie nie podlega procedurze notyfikacji w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597).

Nie zachodzi również konieczność przedstawienia projektu rozporządzenia właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu.

Przedmiot projektu rozporządzenia nie jest regulowany prawem Unii Europejskiej.

Projekt rozporządzenia został zamieszczony w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji w zakładce Rządowy Proces Legislacyjny, stosownie do art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa

(Dz. U. Nr 169, poz. 1414, z późn. zm.) i § 52 ust. 1 uchwały Nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M. P. z 2016 r. poz. 1006 i 1204).

Ocena Skutków Regulacji

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie nadania Naukowej i Akademickiej Sieci Komputerowej statusu państwowego instytutu badawczego **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Marek Zagórski – Sekretarz Stanu w Ministerstwie Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Mariusz Lewandowski – starszy specjalista w Departamencie Prawnym Ministerstwa Cyfryzacji Tel. 22 245 58 20	**Data sporządzenia** 3 kwietnia 2017 r. **Źródło:** Upoważnienie ustawowe art. 21 ust. 5 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2016 r. poz. 371, 1079, 1311 i 2260 oraz z 2017 r. poz. 202) **Nr w wykazie prac:** RD202

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Nadanie statusu państwowego instytut badawczego Naukowej i Akademickiej Sieci Komputerowej ma umożliwić powierzenie instytutowi na podstawie art. 22 pkt 2 lit. a ustawy o instytutach badawczych zadań ciągłych szczególnie ważnych dla planowania i realizacji polityki państwa, których wykonywanie jest niezbędne do zapewnienia bezpieczeństwa publicznego, rozwoju edukacji oraz poprawy jakości życia obywateli, wykonywanych w sposób ciągły, a w szczególności:

1) zapewnienie cyberbezpieczeństwa podmiotom publicznym w zakresie zlecanym i wskazywanym przez ministra właściwego do spraw informatyzacji lub inne organy administracji publicznej, poprzez:
   a) realizację projektów związanych z bezpieczeństwem cyberprzestrzeni Rzeczypospolitej Polskiej,
   b) tworzenie narzędzi do monitorowania sieci bot-net,
   c) utrzymanie operacyjnego centrum zarządzania cyberbezpieczeństwem sfery cywilnej,
   d) rozwój Narodowego Centrum Cyberbezpieczeństwa (NC Cyber);
2) wsparcie w budowie Polski Cyfrowej polegające w szczególności na rozwoju bezpiecznej infrastruktury teleinformatycznej dla nauki (WARMAN) i realizacji projektu Ogólnopolskiej Sieci Edukacyjnej (OSE);
3) prowadzenie badań naukowych i prac rozwojowych ukierunkowanych na ich wdrożenie wspomagających:
   a) rozwój systemów identyfikacji, w tym biometrii,
   b) uczenie maszynowe i sztuczną inteligencję,

c) modelowanie, symulację i optymalizację w systemach sieciowych,
d) cyberbezpieczeństwo,
e) przetwarzanie dużych, zmiennych i różnorodnych danych, w tym w chmurach obliczeniowych,
f) metody analiz sieci społecznych,
g) rozwój „Internetu Rzeczy" (*IoT*),
h) technologię „blockchain";
4) rozwój społeczeństwa informacyjnego i badania nad bezpieczeństwem korzystania z sieci, szczególnie przez dzieci.

Celami projektów związanych z bezpieczeństwem cyberprzestrzeni Rzeczypospolitej Polskiej są: zbudowanie bezpiecznej architektury systemów teleinformatycznych Państwa (składającej się z centrum przetwarzania danych i rozległej sieci komputerowej umożliwiającej bezpieczne łączenie się podmiotów rządowych pomiędzy sobą, z siecią Internet oraz świadczenie usług dla obywateli jak ePUAP, źródło, obywatel.gov.pl.), objęcie monitorowaniem i korelacją zdarzeń kluczowych usług informatycznych zapewniających bezpieczeństwo funkcjonowania Państwa, obywateli i podmiotów gospodarczych, dostarczenie rozwiązań, które umożliwią dostęp do bieżącej informacji o stanie bezpieczeństwa teleinformatycznego niezbędnego do oceny sytuacji i stanu bezpieczeństwa w cyberprzestrzeni w Polsce oraz koordynacji reagowania na incydenty komputerowe na poziomie krajowym. Efektami projektów będą: podniesienie poziomu bezpieczeństwa funkcjonowania podmiotów państwowych poprzez zwiększenie odporności na ataki DDoS, możliwość wykrywania ataków na punktach styków, zwiększenie poufności informacji poprzez implementacje usług zarządzania informacją, podniesienie poziomu bezpieczeństwa funkcjonowania podmiotów państwowych, firm i obywateli w cyberprzestrzeni. Efekty mają być zrealizowane poprzez objęcie monitorowaniem systemów teleinformatycznych wykorzystywanych w procesach kierowania Państwem, a w szczególności służących komunikowaniu się pomiędzy organami władzy publicznej oraz władzą publiczną i społeczeństwem. Ponadto, także przeznaczonych do świadczenia usług kluczowych, które muszą posiadać odporność na zakłócenia wywołane zarówno przez czynniki zewnętrzne, jak i wewnętrzne.

Projekt „tworzenie narzędzi do monitorowania sieci bot-net" polega na analizie działań sieci bot-net oraz stworzeniu narzędzi pozwalających na skuteczne monitorowanie sieci bot-net celem analizy zagrożenia, które mogą spowodować, jej mitygacji a także wykrywaniu nowych, powstających bot-netów oraz monitorowaniu ich działania.

Zadanie „utrzymanie operacyjnego centrum zarządzania cyberbezpieczeństwem sfery cywilnej" związane jest z utrzymaniem centrum w trybie pracy ciągłej 24/7/365. Zadanie związane jest z zarządzeniem incydentami, które będą zgłaszane do Narodowego Centrum

Cyberbezpieczeństwa (znajdującego się w strukturze NASK). Ponadto, zadanie polega na zwiększeniu możliwości reagowania na zmaterializowane zagrożenia w cyberprzestrzeni Rzeczypospolitej Polskiej, tj. utrzymanie zdolności do całodobowej gotowości w zakresie reagowania na incydenty komputerowe, wsparcie jednostek sektorowych, możliwość wykrywania zagrożeń ponadsektorowych. Centrum będzie traktowane jako całodobowy punkt wymiany informacji oraz będzie dostarczać bieżącej informacji o bezpieczeństwie cyberprzestrzeni oraz w poszczególnych sektorach. Mechanizmy zaimplementowane w Centrum pozwolą na alarmowanie w przypadku wystąpienia poważnych cyberataków w cyberprzestrzeni Rzeczypospolitej Polskiej.

Instytut po zmianie statusu będzie wspierał budowę Polski Cyfrowej w szczególności w obszarze rozwoju bezpiecznej infrastruktury teleinformatycznej dla nauki i edukacji.Naukowa i Akademicka Sieć Komputerowa (NASK) już od 2016 roku, na zlecenie Ministra Cyfryzacji, rozpoczęła pilotażowy program, doprowadzenia do szkół łączy o przepustowości 1 Gb/s. Celem tego programu jest:

1) opracowanie i wdrożenie technicznego modelu dostępu do bezpiecznego szerokopasmowego internetu w szkołach podstawowych, gimnazjalnych i ponadgimnazjalnych;
2) uzyskanie danych kosztowych oraz ruchowych do prawidłowego opracowania projektu budowy ogólnopolskiej sieci łączącej szkoły podstawowe i ponadpodstawowe;
3) udostępnienie multimedialnych aplikacji i serwisów o charakterze dydaktycznym.

Wspólna inicjatywa Ministerstwa Cyfryzacji, Ministerstwa Nauki i Szkolnictwa Wyższego oraz Ministerstwa Edukacji Narodowej zakłada podłączenie do szybkich łączy wszystkich jednostek oświatowych w Polsce. Zamierzenie to funkcjonujące pod nazwą Ogólnopolska Sieć Edukacyjna (OSE) jest jednym z kluczowych działań w obszarze rozwoju edukacji i społeczeństwa informacyjnego.

Program ten do chwili obecnej przyniósł wymierne korzyści jednostkom oświaty, które wzięły udział w jego realizacji. Zaowocował też dużą ilością danych dotyczących struktury ruchu generowanego przez jednostki oświaty i jego natężenia, preferencji użytkowników dotyczących wyboru usług edukacyjnych oraz aspektów technicznych funkcjonowania sieci w warunkach szkolnych. W ramach programu, rozwijane są usługi edukacyjne dostępne w tej sieci i tworzone nowe, często rewolucyjne narzędzia edukacyjne.

Projekt OSE został wskazany, jako kluczowy w obszarze Cyfryzacji w Strategii Odpowiedzialnego Rozwoju i zakłada stworzenie sieci dostępu do internetu łączącej wszystkie szkoły w Polsce (ok. 30,5 tys.), co umożliwi wdrożenie innowacyjnych metod nauczania i rozwój edukacji cyfrowej.

Projekt ten wymaga wypracowania przygotowania i późniejszego wdrożenia standardów dla

realizacji tej sieci w szczególności w obszarze bezpieczeństwa infrastruktury. Niezbędne jest więc wsparcie ze strony profesjonalnej jednostki posiadającej odpowiednie kompetencje i potencjał do przeprowadzenia tego typu działań.

Ponadto, ważnym zadaniem NASK jest wspieranie rozwoju społeczeństwa informacyjnego i badań nad bezpieczeństwem korzystania z sieci, szczególnie przez dzieci. W tym celu NASK będzie realizował zadania związane z działalnością informacyjną, profilaktyczną i edukacyjną, wspierając przy tym Ministra Cyfryzacji oraz Ministra Edukacji Narodowej.

Ze względu na zakres dotychczasowej działalności, doświadczenie jak również możliwości organizacyjne i techniczne NASK jest najbardziej odpowiednim podmiotem do realizacji ww. działań. Jednak wykonywanie takich zadań przez NASK w sposób ciągły oraz zapewnienie ich finasowania wymaga zmiany statusu tej jednostki na państwowy instytut badawczy. Umożliwi to powierzenie Instytutowi na podstawie art. 22 pkt 2 lit. a ustawy o instytutach badawczych zadań ciągłych szczególnie ważnego dla planowania i realizacji polityki państwa wskazanych w rozporządzaniu.

Pozwoli to też na wzmocnienie potencjału badawczego i rozwojowego NASK, co przełoży się na sprawniejszą realizację wykonywanych przez tą jednostkę zadań i prac badawczych.

NASK, co do zasady, prowadzi badania naukowe i prace rozwojowe ukierunkowane na ich wdrożenie, które mają wspomagać:

a) rozwój systemów identyfikacji, w tym biometrii,
b) uczenie maszynowe i sztuczną inteligencję,
c) modelowanie, symulację i optymalizację w systemach sieciowych,
d) cyberbezpieczeństwo,
e) przetwarzanie dużych, zmiennych i różnorodnych danych, w tym w chmurach obliczeniowych,
f) metody analiz sieci społecznych,
g) rozwój „Internetu Rzeczy” (IoT),
h) technologię „blockchain”;

Powyższe badania wpływać będą na zwiększenie bezpieczeństwa sieci i systemów informatycznych, w szczególności w obszarach, gdzie przetwarzane są dane osobowe, dane wrażliwe czy też informacje niejawne. Ponadto, prace nad technologią blockchain pozwolą zmniejszyć ryzyko dokonywanych transakcji i uchronić inwestorów przed wszelkiego rodzaju oszustwom i malwersacjom.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Nadanie statusu państwowego instytut badawczego Naukowej i Akademickiej Sieci Komputerowej ma umożliwić powierzenie instytutowi na podstawie art. 22 pkt 2 lit. a ustawy o instytutach badawczych zadań ciągłych szczególnie ważnych dla planowania i realizacji polityki państwa, których wykonywanie jest niezbędne do zapewnienia bezpieczeństwa publicznego, rozwoju edukacji oraz poprawy jakości życia obywateli, wykonywanych w sposób ciągły.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Nie dotyczy

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
	1		

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt został udostępniony na stronie podmiotowej Biuletynu Informacji Publicznej Rządowego Centrum Legislacji w zakładce „Rządowy Proces Legislacyjny" oraz na stronie podmiotowej Biuletynu Informacji Publicznej Ministerstwa Cyfryzacji.

Projekt nie będzie kierowany do konsultacji publicznych, natomiast zostanie skierowany do zaopiniowania przez Polską Akademię Nauk oraz Komitet Rady Ministrów do spraw Cyfryzacji.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Projekt rozporządzenia nie ma wpływu na sektor finansów publicznych,
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Projektowana regulacja nie generuje dodatkowych skutków dla sektora finansów publicznych, a zadania Instytutu będą realizowane głównie w ramach limitu wydatków przewidzianych w ustawie budżetowej na rok 2017 i lata następne, w części budżetowej 27 – Informatyzacja.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
	(dodaj/usuń)	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	0						
	sektor mikro-, małych i średnich przedsiębiorstw	0						
	rodzina, obywatele oraz gospodarstwa domowe	0						
	(dodaj/usuń)	0						
Niemierzalne	(dodaj/usuń)	0						
	(dodaj/usuń)	0						
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń								

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☒ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy

☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☒ inne:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☒ nie dotyczy
Komentarz:	

9. Wpływ na rynek pracy

Projekt rozporządzenia nie ma wpływu na rynek pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	Rozporządzenie umożliwi powierzenie NASK zadań ciągłych szczególnie ważnych dla planowania i realizacji polityki państwa, których wykonywanie jest niezbędne do zapewnienia bezpieczeństwa publicznego, rozwoju edukacji oraz poprawy jakości życia obywateli, wykonywanych w sposób ciągły.

11. Planowane wykonanie przepisów aktu prawnego

Projektowane rozporządzenie wejdzie po upływie 14 dni od dnia ogłoszenia.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Nie dotyczy

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Brak załączników.