Temat nr 9.		
lp.	**Nazwa programu/projektu**	**Opracowanie narzędzi pozwalających na analizę wyrafinowanych technicznie przestępstw popełnianych z użyciem szkodliwego oprogramowania**
1	**Zgłaszający**	**MSWiA – Policja**
2	**Określenie obszarów obronności i bezpieczeństwa państwa**	Przedmiot wpisuje się w następujące priorytetowe obszary technologiczne określone dla 7 strategicznego kierunku badań naukowych i prac rozwojowych Bezpieczeństwo i obronność państwa ustalonego w Krajowym Programie Badań (KPB): – nowoczesne technologie i innowacyjne rozwiązania w zakresie wykrywania, zwalczania i neutralizacji zagrożeń, – technika kryminalistyczna, – nowoczesne technologie lub rozwiązania innowacyjne w sferze bezpieczeństwa teleinformatycznego, ochrony informacji w systemach i sieciach teleinformatycznych oraz narodowej kryptografii. Wdrożenie wyników projektu ma służyć pozyskaniu priorytetowej zdolności operacyjnej służb odpowiedzialnych za bezpieczeństwo do zwalczania cyberprzestępczości, o której, mowa w KPB.
3	**Opis projektu**	Szacuje się, iż tylko w 2015 r. powstało około 144 milionów nowych wariantów szkodliwego oprogramowania, a w chwili obecnej ich łączna liczba wynosi siedemset milionów. Znacząca część powstałych wirusów tworzona jest celem przechwycenia kluczowych informacji, za pomocą których dokonuje się kradzieży pieniędzy zgromadzonych na elektronicznych kontach bankowych, kradzieży danych i wyłudzeń, np. poprzez szyfrowanie zawartości nośników cyfrowych i żądaniu okupu za deszyfrację danych. Warto przy tym podkreślić, że zgodnie z danymi EUROPOL-u w chwili obecnej dochody z tego typu działalności zaczynają przewyższać te pochodzące ze sprzedaży nielegalnych substancji odurzających, a dysproporcja ta będzie zapewne rosła w nadchodzących latach. Straty z tytułu cyberprzestępczości wyniosły w 2017 r. już ponad biliard dolarów amerykańskich i w dokumentach strategicznych UE oraz wielu państw, cyberprzestępczość wskazywana jest jako jedno z priorytetowych zagrożeń dla bezpieczeństwa państwa i jego obywateli. Dlatego też, wraz ze wzrostem wyrafinowania technik stosowanych przez autorów szkodliwego oprogramowania oraz powstających w rezultacie ich działania szkód finansowych, konieczne jest wyszkolenie i wyposażenie biegłych badań informatycznych w umiejętności oraz narzędzia pozwalające na analizę i wykrywanie tego typu przestępstw. Wymaganym jest w ramach projektu opracowanie narzędzi umożliwiających: – analizę dużych zbiorów danych (logów systemowych, dzienników połączeń/billingów, baz danych, danych pochodzących z routerów, zapór sieciowych), ich wizualizację i badanie korelacji. Narzędzia te powinny pozwolić m.in. na wykrywanie typowych zachowań w oparciu o predefiniowane, a możliwe do dalszej rozbudowy, wzorce (np. próby nieautoryzowanego logowania, podniesienia uprawnień, powtarzane cyklicznie akcje, nietypowe połączenia). Zasadnym jest w tym celu wykorzystać metody sztucznej inteligencji i eksploracji danych: heurystyczne przeszukiwanie, w tym algorytmy ewolucyjne, automatyczne systemy wnioskujące wykorzystujące logikę rozmytą i algorytmy uczenia oraz metody klasteryzacji i klasyfikacji danych oraz rozpoznawanie wzorców. – zautomatyzowaną analizę wraz z innymi plikami w wyizolowanym środowisku (sandbox). Narzędzia powinny mieć zaimplementowane skrypty utrudniające wykrywanie przez szkodliwe oprogramowanie prób dokonania analizy ich kodu (antisandbox techniques). Umożliwi

		to opracowanie raportów zawierających informacje o serwerach, z którymi oprogramowanie może nawiązywać połączenie jak \i o tworzonych plikach, modyfikacjach rejestrów czy innych kluczowych ustawieniach systemu operacyjnego. W ramach cech opracowywanego systemu sandboxowego wymagana jest implementacja m.in. następujących funkcjonalności: ▪ możliwość analizy zaciemnionych skryptów VBA, ▪ umożliwienie analizy skompilowanych plików zapisanych w formacie Adobe flash (swf), ▪ tworzenie chronologicznego zestawienia szczegółów technicznych działania szkodliwego oprogramowania (obejmującego kolejno wykonywane operacje obejmującego wywołania API, rejestr, pamięć systemową), ▪ rozpoznawania tekstu zapisanego w formatach graficznych zawartych w szkodliwym oprogramowaniu (ransomware), ▪ implementacja algorytmów pozwalających na wykrywanie oprogramowania używającego steganografii do przesyłania informacji, ▪ możliwość tworzenia własnych rodzajów skryptów symulujących działania użytkownika, ▪ niezależność piaskownicy od użytego hiperwizora, ▪ możliwość analizy programów operujących na poziomie jądra systemu (kernel mode). – stanowiska badawcze powinny zostać wyposażone w oprogramowanie pozwalające na analizę aktywności użytkowników pod kątem artefaktów pozostawionych w trakcie łączenia się z siecią Internet (historia odwiedzanych stron internetowych, prowadzonych rozmów przy użyciu komunikatorów, wyszukiwanych treści). Ponadto policyjni biegli i specjaliści z zakresu badań informatycznych powinni zostać przeszkoleni z zakresu zaawansowanych technik analizy śladów pozostawionych przez szkodliwe oprogramowanie, interpretacji logów. <u>Oczekiwane efekty</u>: – opracowanie procedury postępowania dla organów ścigania w sprawach, w których posłużono się szkodliwym oprogramowaniem. Szczególny nacisk powinien być położony na kwestię zabezpieczania na miejscu zdarzenia tzw. „danych ulotnych” w postaci logów systemowych, zrzutów pamięci operacyjnej itp. Przedmiotowe działania przełożą się na wzrost wykrywalności sprawców przestępstw tego typu, co pozwoli, w dalszej perspektywie, na skuteczniejsze odzyskiwanie utraconego mienia, – opracowanie procedury dotyczących badań nośników cyfrowych w przypadku popełnienia przestępstwa z użyciem szkodliwego oprogramowania. Pozwoli to organom ścigania na sporządzenie opinii kryminalistycznej, która na etapie postępowania przygotowawczego, a następnie sądowego, będzie wykorzystana jako wartościowy środek dowodowy, – opracowanie narzędzi, które stanowić będą wyposażenie pracowni badań informatycznych/wydziałów dw. z cyberprzestępczością w oprogramowanie pozwalające na kryminalistyczne badania zachowania podejrzanych zbiorów danych oraz analizę dużej ilości logów/baz danych, szerokiego spektrum artefaktów w sposób umożliwiający wykrywanie anomalii mogących świadczyć o popełnianych przestępstwach. Pozwoli to na kompleksową analizę szkodliwego oprogramowania, od momentu próby jego identyfikacji w działającym systemie (przy użyciu utworzonych systemów wykrywania anomalii) do jego późniejszej analizy zarówno statycznej jak i dynamicznej w utworzonych środowiskach testowych. – stworzenie wspólnej bazy zawierającej informacje o postępowaniach w trakcie których zidentyfikowano szkodliwe oprogramowania, co pozwoli na ustalenie spraw, w których posłużono się tą samą metodą/oprogramowaniem. Pomoże to w dalszej perspektywie w zwalczaniu podobnych przestępstw, jak również umożliwi wypracowanie odpowiednich procedur zapobiegania ich popełnianiu, opracowanie nowych standardów współpracy i komunikacji z polskimi organizacjami pozarządowymi i instytucjami naukowymi zajmującymi się bezpieczeństwem teleinformatycznym kraju. Pozwoli to na szybsze i skuteczniejsze reagowanie przez organy ścigania na zagrożenia

		pojawiające się w zasobach polskiego Internetu, a także pozwoli na korzystanie z know-how udostępnianego przez wyspecjalizowane agendy (np. zespoły CERT, bankowe zespoły bezpieczeństwa).
4	**Określenie celu głównego i celów szczegółowych oraz ich relacji do celów innych programów i projektów, a także wskazanie planowanych do uzyskania poziomów gotowości technologii, o których mowa w załączniku do rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 4 stycznia 2011 r. w sprawie sposobu zarządzania przez Narodowe Centrum Badań i Rozwoju realizacją badań naukowych lub prac rozwojowych na rzecz obronności i bezpieczeństwa państwa, w tym dla technologii krytycznych o znaczeniu determinującym powodzenie całego programu lub projektu**	Celem głównym jest opracowanie narzędzi umożliwiających zautomatyzowaną analizę behawioralną szkodliwego oprogramowania, jak również wizualizację i korelację danych z systemów informatycznych oraz wykrywanie anomalii w logach systemowych oraz aktywnych procesach świadczących o popełnieniu przestępstwa. Cele szczegółowe: 1. opracowanie narzędzi umożliwiających automatyczną analizę różnorodnych zbiorów danych, zabezpieczonych w związku z ujawnieniem przez organy ścigania przestępstw popełnionych z użyciem szkodliwego oprogramowania; 2. opracowanie systemu umożliwiającego w sposób zautomatyzowany analizę behawioralną programów w oparciu o wyizolowane środowisko (sandbox); 3. opracowanie systemu wykrywania w sposób zautomatyzowany anomalii pozwalającego na instalacje zestawu „czujników" w środowiskach zwirtualizowanych/rzeczywistych, celem monitorowania aktywności systemu oraz raportowania podejrzanej aktywności (analiza na podstawie sygnatur/ reguł heurystycznych); 4. przetestowanie opracowanych narzędzi w warunkach rzeczywistych, co pozwoli na ich wykorzystanie po zakończeniu realizacji projektu; 5. przeprowadzenie szkoleń i spotkań roboczych, związanych z obsługą opracowanych narzędzi w obszarze identyfikacji i ujawniania śladów przestępstw popełnianych drogą elektroniczną z użyciem szkodliwego oprogramowania; 6. utworzenie bazy zawierającej informacje o postępowaniach, w trakcie których zidentyfikowano szkodliwe oprogramowanie, co pozwoli na powiązanie spraw, w których posłużono się tą samą metodą przestępstwa; 7. wymiana informacji z innymi ośrodkami rządowymi i komercyjnymi w zakresie związanym z analizą "malware" (np. zespołami CRT/producentami rozwiązań antywirusowych, bankowymi zespołami bezpieczeństwa). Powiązania z dokumentami strategicznymi: 1. Europejska Agenda Bezpieczeństwa na lata 2015-2020. Priorytet III - zwalczanie cyberprzestępczości: – zapewnienie budowania zdolności w zakresie bezpieczeństwa cybernetycznego wśród właściwych organów państw członkowskich, – wsparcie współpracy między organami ścigania i organami odpowiedzialnymi za bezpieczeństwo cybernetyczne, – ustrukturyzowanie wspólnych wysiłków publiczno-prywatnych na rzecz zwalczania przestępczości w Internecie. 2. Priorytety i Zadania Priorytetowe Komendanta Głównego Policji na lata 2016-2018: – pkt. 2.6 "Stworzenie ogólnopolskiego systemu wymiany i koordynacji informacji w zakresie cyberprzestępczości", – pkt. 2.7 „Rozwój technologiczny komórek zwalczających cyberprzestępczość (np. poprzez tworzenie laboratoriów specjalistycznych do analiz oprogramowania i sprzętu teleinformatycznego), – pkt. 6.9 „Organizacja i prowadzenie kursów specjalistycznych w obszarze zwalczania cyberprzestępczości. Technologią krytyczną projektu jest opracowanie systemu sandboxowego/piaskownicy. **Oczekiwany poziom gotowości technologicznej: IX**

<table>
<tr><td>5</td><td>Określenie, czy program strategiczny, program lub projekt ma być w całości realizowany przez jednego wykonawcę;</td><td>Projekt ma być w całości realizowany przez jednego Wykonawcę. Wykonawcą może być konsorcjum naukowe lub podmiot przemysłowy.</td></tr>
<tr><td>6</td><td>Określenie w formie harmonogramu, pożądanych terminów realizacji projektu, w tym jego etapów w szczególności podlegających rozliczeniu w ramach procesu nadzoru</td><td>
Harmonogram wykonania projektu powinien w szczególności uwzględniać realizację następujących zadań:

opracowanie narzędzi umożliwiających automatyczną analizę różnorodnych zbiorów danych, zabezpieczonych w związku z ujawnieniem przez organy ścigania przestępstw popełnionych z użyciem szkodliwego oprogramowania;
opracowanie systemu umożliwiającego w sposób zautomatyzowany analizę behawioralną programów w oparciu o wyizolowane środowisko (sandbox);
opracowanie systemu wykrywania w sposób zautomatyzowany anomalii pozwalającego na instalacje zestawu „czujników” w środowiskach zwirtualizowanych/rzeczywistych, celem monitorowania aktywności systemu oraz raportowania podejrzanej aktywności (analiza na podstawie sygnatur/ reguł heurystycznych);
przetestowanie opracowanych narzędzi w warunkach rzeczywistych, co pozwoli na ich wykorzystanie po zakończeniu realizacji projektu;
przeprowadzenie szkoleń i spotkań roboczych, związanych z obsługą opracowanych narzędzi w obszarze identyfikacji i ujawniania śladów przestępstw popełnianych drogą elektroniczną z użyciem szkodliwego oprogramowania;
utworzenie bazy zawierającej informacje o postępowaniach, w trakcie których zidentyfikowano szkodliwe oprogramowanie, co pozwoli na powiązanie spraw, w których posłużono się tą samą metodą przestępstwa;

<table>
<tr><th></th><th>Kamień milowy</th><th>Maksymalny termin osiągnięcia kamienia milowego (w miesiącach)</th></tr>
<tr><td colspan="3">BADANIA NAUKOWE</td></tr>
<tr><td>1.</td><td>Zatwierdzenie przez gestora programu badań.</td><td>3</td></tr>
<tr><td>2.</td><td>Zatwierdzenie przez Gestora dokumentacji technicznej opracowanego rozwiązania.</td><td>12</td></tr>
<tr><td colspan="3">PRACE ROZWOJOWE</td></tr>
<tr><td>3.</td><td>Zatwierdzenie przez gestora procedur wykonawczych.</td><td>30</td></tr>
<tr><td>4.</td><td>Zatwierdzenie przez gestora dokumentacji technicznej opracowanego rozwiązania.</td><td>36</td></tr>
</table>
Pożądany czas trwania realizacji projektu to 36 miesięcy

Projekt powinien być realizowany etapami, a każdy z etapów kończyć się osiągnięciem kolejnego poziomu gotowości technologii (PGT) zgodnie z wymogami określonymi w załączniku do rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 4 stycznia 2011 r. w sprawie w sprawie sposobu zarządzania przez Narodowe Centrum Badań i Rozwoju realizacją badań naukowych lub prac rozwojowych na rzecz obronności i bezpieczeństwa państwa (Dz. U. 2011 Nr 18, poz. 91).
</td></tr>
</table>

		Pozytywny wynik etapów badań naukowych (zakończonych uzyskaniem VI PGT) potwierdzający możliwość skutecznego stosowania technologii determinującej powodzenie projektu oraz osiągniecie kluczowych funkcjonalności i parametrów zawartych w opisie projektu wraz z analizą możliwości i koncepcją jej rozwoju jest warunkiem kontynuacji projektu i rozpoczęcia fazy rozwojowej. Szczegółowy harmonogram realizacji projektu zaproponuje wnioskodawca we wniosku o dofinansowanie projektu.
7	**Docelowy, główny użytkownik końcowy (gestor)**	**Policja**, Siły Zbrojne, ABW, Straż Graniczna.
8	**Ustalenie planu finansowego, w tym źródeł finansowania**	Projekt będzie finansowany ze środków NCBR, przewidzianych na finansowanie badań naukowych i prac rozwojowych na rzecz bezpieczeństwa i obronności i państwa. (dotacja celowa) Wnioskodawca przedstawi we wniosku o dofinasowanie kalkulację kosztów realizacji projektu z podziałem na poszczególne lata. Planowany koszt realizacji projektu może być modyfikowany na podstawie wniosków złożonych przez wnioskodawców i w trakcie negocjacji przed zawarciem umowy.
9	**Ustalenie sposobu realizacji i zarządzania, w szczególności w zakresie organizacji kontroli, nadzoru i odbioru prac**	Wykonawca będzie realizował projekt i zarządzał nim w oparciu o uznaną metodykę zarządzania projektami np. PRINCE2. Dyrektor Centrum będzie sprawował nadzór nad realizacją projektu i może prowadzić kontrolę zgodnie z ustawą o NCBR, rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 4 stycznia 2011 r. w sprawie sposobu zarządzania przez Narodowe Centrum Badań i Rozwoju realizacją badań naukowych lub prac rozwojowych na rzecz obronności i bezpieczeństwa państwa (Dz. U. 2011 Nr 18, poz. 91) oraz wewnętrznymi regulacjami NCBR w tym zakresie. Nadzór nad realizacją projektu będzie prowadzony przez Zespół Nadzorujący, powołany przez Dyrektora NCBR. W skład zespołu nadzorującego wchodzą przedstawiciele ministra właściwego do spraw wewnętrznych, którzy pełnią w nim rolę ekspertów merytorycznych. Ekspertem wiodącym w zespole nadzorującym będzie przedstawiciel Ministra Spraw Wewnętrznych i Administracji. Proponowanym ekspertem wiodącym w zespole nadzorującym projekt w NCBR jest NCBR jest przedstawiciel Laboratorium Kryminalistycznego KWP w Rzeszowie. Proponowanym podmiotem odpowiedzialnym za testowanie rozwiązań u przyszłego użytkownika w warunkach zbliżonych do operacyjnych lub/i w warunkach rzeczywistych - uprawniony do ustalenia programu badań i testów oraz innych spraw związanych z testowaniem jest Policja. Dyrektor Centrum po uzyskaniu końcowej oceny merytorycznej projektu wykonanej przez Komitet Sterujący NCBR, dokona przyjęcia i oceny wyników projektu poprzez uznanie umowy o wykonanie i finasowanie projektu za wykonaną lub niewykonaną.

10	**Prawa własności intelektualnej**	Właściciel PWI – SP Właścicielem wynalazków, wzorów użytkowych i wzorów przemysłowych oraz autorskich praw majątkowych powstałych w wyniku wykonania Projektu zwanych dalej prawami własności intelektualnych (PWI) jest Skarb Państwa reprezentowany przez Komendanta Głównego Policji. Wykonawca będzie zobowiązany, na podstawie zawartej umowy o wykonanie i finasowanie projektu, do udzielenia licencji w zakresie odpowiadającym art. 32 ust. 3a powyższej ustawy na rozwiązania posiadane przez Wnioskodawcę lub przez niego nabyte, które ramach finansowania zostaną wykorzystane w celu realizacji projektu, a bez których nie byłoby możliwe korzystanie z rozwiązań powstałych w wyniku realizacji projektu. Wykonawca będzie zobowiązany do przeniesienia na Skarb Państwa własności prototypów oraz demonstratorów powstałych w wyniku wykonania projektu, bez prawa do dodatkowego wynagrodzenia (tj. w ramach otrzymanego na podstawie umowy przez Wykonawcę finansowania), na wyraźne żądanie Skarbu Państwa zgłoszone w terminie określonym w umowie o wykonanie i finansowanie projektu. Wykonawca projektu, na żądanie Skarbu Państwa lub Centrum, będzie zobowiązany przekazać wszelką dokumentację dotyczącą PWI oraz rozwiązań posiadanych przez Wnioskodawcę lub przez niego nabytych w ramach finansowania, które zostaną wykorzystane w celu realizacji projektu, a bez których nie byłoby możliwe korzystanie z rozwiązań powstałych w wyniku realizacji projektu, w szczególności ich podstawowe założenia, opis techniczny, specyfikacje oraz wizualizacje, kody źródłowe, wynikowe, maszynowe i inne, dokumentację projektową, techniczną i eksploatacyjną.
11	**Zmiany w założeniach**	Niniejsze założenia do programu (projektu) mogą być modyfikowane przez Komitet Sterujący do spraw badań naukowych i prac rozwojowych na rzecz bezpieczeństwa i obronności państwa przy realizacji jego zadań oraz przez Dyrektora Centrum na etapie inicjowania programu (projektu) oraz w trakcie nadzoru nad realizacją umowy o wykonanie i finasowanie projektu (projektów w ramach programu) na podstawie opinii, rekomendacji Zespołu Nadzorującego lub Komitetu Sterującego, a w razie potrzeby ekspertów i w takim przypadku zmiany te nie wymagają uzgadniania z Ministrem Obrony Narodowej i ministrem właściwym do spraw wewnętrznych, którzy posiadają swoich przedstawicieli w Komitecie Sterującym.