Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA)

COM(2010) 521 wersja ostateczna

(2011/C 107/12)

Sprawozdawca: **Peter MORGAN**

Dnia 19 października 2010 r. Rada, działając na podstawie art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), postanowiła zasięgnąć opinii Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie

wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA)

COM(2010) 521 wersja ostateczna.

Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego, której powierzono przygotowanie prac Komitetu w tej sprawie, przyjęła swoją opinię 2 lutego 2011 r.

Na 469. sesji plenarnej w dniach 16–17 lutego 2011 r. (posiedzenie z 17 lutego) Europejski Komitet Ekonomiczno-Społeczny 173 głosami – 5 osób wstrzymało się od głosu – przyjął następującą opinię:

1. **Wnioski i zalecenia**

1.1 EKES jest świadom obecnego stopnia zależności społeczeństwa obywatelskiego od usług internetowych, a także jego względnej niewiedzy na temat bezpieczeństwa cybernetycznego. EKES uważa, że Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) odpowiada za udzielanie państwom członkowskim i operatorom pomocy w zakresie podnoszenia ogólnych standardów bezpieczeństwa w trosce o to, by wszyscy użytkownicy internetu podejmowali kroki konieczne do zapewnienia swego osobistego bezpieczeństwa cybernetycznego.

1.2 EKES popiera zatem propozycję rozbudowania agencji ENISA w celu zapewnienia wysokiego poziomu bezpieczeństwa sieci i informacji w Unii oraz podnoszenia świadomości i rozwijania w społeczeństwie kultury bezpieczeństwa sieci i informacji na rzecz obywateli, konsumentów, przedsiębiorstw oraz organizacji sektora publicznego w Unii, a tym samym w celu przyczyniania się do sprawnego funkcjonowania rynku wewnętrznego.

1.3 Zadania ENISA mają istotne znaczenie dla bezpiecznego rozwoju infrastruktury sieciowej rządów, przemysłu, handlu i społeczeństwa obywatelskiego UE. EKES oczekuje, że Komisja Europejska ustanowi dla agencji ENISA najwyższe normy eksploatacyjne i że będzie monitorowała jej funkcjonowanie w kontekście zmieniających się i wciąż nowych zagrożeń bezpieczeństwa cybernetycznego.

1.4 Realizacja strategii cybernetycznych przedstawionych przez NATO, Europol i Komisję Europejską zależy od skutecznej współpracy z państwami członkowskimi, które mają już wiele różnorodnych agencji wewnętrznych ds. bezpieczeństwa cybernetycznego. Strategie NATO i Europolu mają być proaktywne i operacyjne. W strategii Komisji Europejskiej agencja ENISA wyraźnie jest istotną częścią złożonego systemu agencji i misji mających na celu ochronę krytycznej infrastruktury informatycznej (Critical Information Infrastructure Protection, CIIP). Choć w nowym rozporządzeniu nie zaproponowano roli operacyjnej dla agencji ENISA, EKES nadal uważa, że to w pierwszym rzędzie ENISA jest odpowiedzialna za CIIP w społeczeństwie obywatelskim UE.

1.5 Odpowiedzialność operacyjna za bezpieczeństwo cybernetyczne na szczeblu państw członkowskich spoczywa na tychże państwach, niemniej standardy ochrony krytycznej infrastruktury informatycznej (CIIP) w 27 państwach członkowskich są wyraźnie zróżnicowane. Zadaniem agencji ENISA jest więc zwiększenie bezpieczeństwa cybernetycznego mniej zaawansowanych pod tym względem państw członkowskich do akceptowalnego poziomu. Agencja musi zapewnić współpracę między państwami członkowskimi oraz pomóc im w stosowaniu sprawdzonych rozwiązań. W kontekście zagrożeń transgranicznych rola ENISA musi polegać zarówno na ostrzeganiu, jak i na działaniach prewencyjnych.

1.6 ENISA będzie również musiała włączyć się we współpracę międzynarodową z władzami spoza UE. Współpraca ta będzie miała charakter wysoce polityczny i będzie dotyczyła wielu dziedzin działań UE. Niemniej EKES uważa, że ENISA musi znaleźć odpowiednie miejsce na scenie międzynarodowej.

1.7 Komitet uważa, że agencja ENISA może odgrywać bardzo cenną rolę, uczestnicząc w projektach badawczych w dziedzinie bezpieczeństwa, a także je inicjując.

1.8 Jeśli chodzi o ramy oceny skutków, EKES obecnie nie poprze pełnej realizacji wariantów 4 i 5, które przeobraziłyby ENISA w agencję operacyjną. Bezpieczeństwo cybernetyczne jest tak poważnym problemem, a liczba zagrożeń rośnie tak szybko,

że państwa członkowskie muszą zachować zdolność proaktywnego przeciwdziałania zagrożeniom. Rozwój agencji operacyjnych UE zazwyczaj prowadzi do obniżenia umiejętności w państwach członkowskich. W dziedzinie bezpieczeństwa cybernetycznego sytuacja jest odwrotna, gdyż konieczne jest zwiększenie zdolności państw członkowskich.

1.9 EKES rozumie stanowisko Komisji, która uważa, że zadania agencji ENISA powinny być ściśle określone i kontrolowane i że należy przyznać jej odpowiednie środki. Niemniej EKES obawia się, że pięcioletnia kadencja agencji ENISA może ograniczyć prace nad projektami długofalowymi i zagrozić rozwojowi zasobów ludzkich i zasobów wiedzy do dyspozycji agencji. Ta dosyć mała agencja będzie zajmować się poważnym i wciąż narastającym problemem. Ze względu na zakres i skalę swych zadań agencja ENISA będzie musiała zatrudniać zespoły specjalistów. Będzie ona wykonywała różne prace, wywiązywała się z krótkoterminowych zadań, jak i realizowała projekty długofalowe. W związku z tym EKES wolałby, by mandat agencji ENISA był dynamiczny i otwarty i by był regularnie potwierdzany na podstawie ocen okresowych. Dzięki temu zasoby mogłyby być przydzielane stopniowo i w uzasadnionych przypadkach.

2. **Wstęp**

2.1 Niniejsza opinia dotyczy rozporządzenia mającego na celu dalszy rozwój agencji ENISA.

2.2 Komisja przedstawiła swą pierwszą propozycję podejścia politycznego do bezpieczeństwa sieci i informacji w komunikacie z 2001 r. (COM(2001) 298 wersja ostateczna), w sprawie którego Daniel Retureau sporządził wyczerpującą opinię ([1]).

2.3 Następnie Komisja zaproponowała rozporządzenie w celu ustanowienia agencji ENISA (COM(2003) 63 wersja ostateczna). Opinia EKES-u ([2]) w sprawie tego rozporządzenia została opracowana przez Görana Lagerholma. Agencja została faktycznie ustanowiona na mocy rozporządzenia (WE) nr 460/2004.

2.4 Wraz z gwałtownym wzrostem liczby użytkowników internetu bezpieczeństwo informacji stawało się coraz poważniejszym problemem. W 2006 r. Komisja wydała komunikat przedstawiający strategię na rzecz bezpiecznego społeczeństwa informacyjnego (COM(2006) 251 wersja ostateczna), a Antonello Pezzini sporządził opinię w tej sprawie ([3]).

2.5 Gdy obawy o bezpieczeństwo informacji jeszcze bardziej się nasiliły, Komisja wydała w 2009 r. wniosek w sprawie ochrony krytycznej infrastruktury informatycznej (COM(2009) 149 wersja ostateczna). Thomas McDonogh sporządził opinię ([4]), która została przyjęta na sesji plenarnej EKES-u w grudniu 2009 r.

([1]) Dz.U. C 48 z 21.2.2002, s. 33.
([2]) Dz.U. C 220 z 16.9.2003, s. 33.
([3]) Dz.U. C 97 z 28.4.2007, s. 21.
([4]) Dz.U. C 255 z 22.9.2010, s. 98.

2.6 Teraz proponuje się wzmocnienie i udoskonalenie agencji ENISA w celu zapewnienia wysokiego poziomu bezpieczeństwa sieci i informacji w Unii oraz podnoszenia świadomości i rozwijania w społeczeństwie kultury bezpieczeństwa sieci i informacji na rzecz obywateli, konsumentów, przedsiębiorstw oraz organizacji sektora publicznego w Unii, a tym samym w celu przyczyniania się do sprawnego funkcjonowania rynku wewnętrznego.

2.7 Niemniej ENISA nie jest jedyną agencją ds. bezpieczeństwa, jaką planuje się z myślą o cyberprzestrzeni UE. Odpowiedzialność za reagowanie na wojny cybernetyczne i cyberterroryzm spoczywa na wojsku. NATO, które jest główną agencją zajmującą się tą tematyką. Zgodnie z jego nową koncepcją strategiczną wydaną w listopadzie 2010 r. w Lizbonie (zob. dokument na stronie: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf) NATO „rozwinie jeszcze bardziej swą zdolność zapobiegania atakom cybernetycznym, a także ich wykrywania, obrony przed nimi i odzyskiwania danych, między innymi poprzez wykorzystanie swego procesu planowania, by zwiększyć i skoordynować umiejętności obrony cybernetycznej na szczeblu krajowym, objęcie wszystkich organów NATO scentralizowaną ochroną cybernetyczną i lepsze skoordynowanie wiedzy, ostrzegania i reagowania NATO z państwami członkowskimi".

2.8 Po ataku cybernetycznym na Estonię w 2007 r., 14 maja 2008 r. powołano oficjalnie Centrum Doskonałości ds. Współpracy w Dziedzinie Obrony przed Atakami Cybernetycznymi (CCD COE), tak by zwiększyć zdolność NATO do obrony cybernetycznej. Centrum mieści się w Tallinie w Estonii i jest strukturą międzynarodową, której działalność finansują obecnie Estonia, Łotwa, Litwa, Niemcy, Węgry, Włochy, Słowacja i Hiszpania.

2.9 Zwalczanie przestępczości elektronicznej na szczeblu UE jest zadaniem Europolu. Poniżej przytoczony został fragment pisemnej opinii przedstawionej Izbie Lordów przez Europol (zob. http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68we05.htm): „Rzecz jasna, organy ścigania muszą dotrzymać kroku rozwojowi technologicznemu przestępców, by zapewnić skuteczne zapobieganie popełnianym przez nich przestępstwom lub ich skuteczne wykrywanie. Ponadto, wziąwszy pod uwagę ponadgraniczny charakter nowoczesnych technologii, w całym UE zdolności w tym względzie muszą być na równie wysokim poziomie, by nie dopuścić do powstania »słabych punktów«, w których zaawansowana technologicznie przestępczość mogłaby się bezkarnie rozwijać. W UE poziom rozwoju tych zdolności jest bardzo zróżnicowany. W gruncie rzeczy mamy do czynienia z asymetrycznym rozwojem, gdyż niektóre państwa członkowskie czynią szybkie postępy w niektórych obszarach, podczas gdy inne pozostają w tyle pod względem technologicznym. W związku z tym konieczne jest stworzenie centralnych służb, które pomagałyby wszystkim państwom członkowskim w koordynacji wspólnych działań, propagowaniu normalizacji podejść i standardów jakości, a także identyfikacji i wymianie sprawdzonych rozwiązań. Tylko w ten sposób można zapewnić jednolite egzekwowanie prawa UE w celu zwalczania zaawansowanej technologicznie przestępczości".

2.10 Centrum ds. Przestępczości Zaawansowanej Technologicznie (High Tech Crime Centre, HTCC) zostało utworzone w ramach Europolu w 2002 r. Jest to stosunkowo niewielka jednostka, lecz jako główny filar prac Europolu w tej dziedzinie w przyszłości zapewne się powiększy. Centrum odgrywa istotną rolę w zakresie koordynacji, wsparcia operacyjnego, analizy strategicznej i kształcenia. Szczególnie duże znaczenie ma funkcja szkoleniowa. Europol powołał ponadto europejską platformę walki z cyberprzestępczością (European Cyber Crime Platform, ECCP), która zajmuje się głównie następującymi zagadnieniami:

— *Internet Crime Reporting Online System* (I-CROS) – internetowy system sprawozdawczości o cyberprzestępstwach;

— *Analysis Work File* (Cyborg) – grupa zajmująca się analizą;

— *Internet and Forensic Expertise recipient* (I-FOREX) – system gromadzenia specjalistycznej wiedzy kryminalistycznej z zakresu cyberprzestępczości.

2.11 Strategia bezpieczeństwa cybernetycznego UE została przedstawiona w rozdziale europejskiej agendy cyfrowej poświęconym zaufaniu i bezpieczeństwu. Wyzwania opisano w następujący sposób:

„Do tej pory internet był stosunkowo bezpieczny, odporny i stabilny, ale sieci i komputery użytkowników końcowych pozostają narażone na szereg coraz bardziej zróżnicowanych zagrożeń. W ostatnich latach spam rozwinął się do tego stopnia, że znacznie spowalnia przesyłanie wiadomości elektronicznych. Szacuje się, że między 80 a 98 % wszystkich wysyłanych wiadomości to wiadomości typu spam. W ten sposób rozprzestrzenia się wiele wirusów i złośliwego oprogramowania. Coraz częściej występują przypadki kradzieży tożsamości i oszustw internetowych. Ataki stają się coraz bardziej wyrafinowane (trojany, botnety itp.). Często motywacja jest finansowa. Czasami ataki następują z przyczyn politycznych, jak np. niedawne ataki w Estonii, na Litwie i w Gruzji".

2.12 W ramach agendy Komisja zobowiązuje się podjąć następujące działania:

Główne działanie 6: Przedstawienie w 2010 r. środków ukierunkowanych na **prowadzenie na wysokim szczeblu udoskonalonej polityki w zakresie bezpieczeństwa sieci i informacji**, w tym inicjatyw ustawodawczych, takich jak np. unowocześnienie agencji ENISA, a także przedstawienie środków umożliwiających szybsze reagowanie na wypadek ataków cybernetycznych, w tym zespołów ds. reagowania kryzysowego w dziedzinie informatycznej (Computer Emergency Response Team, CERT) dla instytucji UE;

Główne działanie 7: Przedstawienie do 2010 r. środków, w tym inicjatyw ustawodawczych, ukierunkowanych na **zwalczanie ataków cybernetycznych na systemy informatyczne** oraz powiązanych przepisów dotyczących jurysdykcji w cyberprzestrzeni na szczeblu europejskim i międzynarodowym (do 2013 r.).

2.13 W komunikacie z listopada 2010 r. (COM(2010) 673 wersja ostateczna) Komisja rozwinęła agendę, przedstawiając w zarysie strategię bezpieczeństwa wewnętrznego UE. Strategia ta ma pięć celów, z których trzecim jest podniesienie poziomu bezpieczeństwa obywateli i przedsiębiorstw w cyberprzestrzeni. Przewidziano trzy programy działania, a szczegóły tych działań są przedstawione w następującej tabeli (źródło: komunikat Komisji: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:PL:pdf).:

CELE I DZIAŁANIA	ODPOWIEDZIALNY	CZAS
CEL 3: Podniesienie poziomu ochrony obywateli i przedsiębiorstw w cyberprzestrzeni		
Działanie 1: Budowa zdolności w zakresie egzekwowania prawa i sądownictwa		
Utworzenie unijnego centrum ds. walki z cyberprzestępczością	Przedmiot studium wykonalności, które COM ukończy w 2011 r.	2013
Rozwój potencjału dochodzeniowo-śledczego i ścigania przestępstw w dziedzinie cyberprzestępczości	państwa członkowskie wraz z Europejskim Kolegium Policyjnym (CEPOL), Europolem i Eurojustem	2013
Działanie 2: Współpraca z przemysłem w celu wzmacniania pozycji obywateli i ich ochrony		
Stworzenie mechanizmów dla zgłaszania zawiadomień o popełnieniu cyberprzestępstwa i wyposażenie obywateli w informacje na temat bezpieczeństwa cybernetycznego i cyberprzestępczości	państwa członkowskie, Komisja, Europol, **ENISA** oraz sektor prywatny	Procedura w toku
Wytyczne dotyczące współpracy w zwalczaniu nielegalnych treści w Internecie	Komisja wraz z państwami członkowskimi i sektorem prywatnym	2011
Działanie 3: Poprawa zdolności reagowania na ataki cybernetyczne		
Utworzenie sieci zespołów ds. reagowania kryzysowego w dziedzinie informatycznej w każdym państwie członkowskim oraz jednego takiego zespołu dla instytucji UE, jak również opracowanie krajowych planów awaryjnych i przeprowadzanie ćwiczeń w zakresie reagowania na zagrożenia i odzyskiwania danych	państwa członkowskie i instytucje UE wraz z **ENISA**	2012
Utworzenie europejskiego systemu ostrzegania i wymiany informacji (EISAS)	państwa członkowskie wraz z Komisją i **ENISA**	2013

2.14 Realizacja strategii cybernetycznych przedstawionych przez NATO, Europol i Komisję Europejską zależy od skutecznej współpracy z państwami członkowskimi, które mają już wiele różnych agencji wewnętrznych ds. bezpieczeństwa cybernetycznego. Strategie NATO i Europolu mają być proaktywne i operacyjne. W strategii Komisji Europejskiej ENISA jest ważnym elementem skomplikowanego i rozbudowanego systemu agencji i misji mających na celu ochronę krytycznej infrastruktury informatycznej (CIIP). Ponadto – choć w nowym rozporządzeniu nie przyznano ENISA roli operacyjnej – EKES nadal uważa ENISA za agencję, która w pierwszym rzędzie ponosi odpowiedzialność za ochronę krytycznej infrastruktury informatycznej (CIIP) wobec społeczeństwa obywatelskiego UE.

3. **Wniosek w sprawie agencji ENISA**

3.1 Problem, któremu ma zaradzić agencja ENISA, powodowany jest przez siedem czynników:

(1) rozdrobnienie i zróżnicowanie podejść krajowych,

(2) ograniczona zdolność Europy do wczesnego ostrzegania i reagowania,

(3) brak wiarygodnych danych i ograniczona wiedza na temat ewoluujących problemów,

(4) brak świadomości zagrożeń i wyzwań związanych z bezpieczeństwem sieci i informacji,

(5) międzynarodowy wymiar problemów związanych z bezpieczeństwem sieci i informacji,

(6) zapotrzebowanie na modele współpracy zapewniające właściwą realizację polityki,

(7) potrzeba skuteczniejszych działań przeciwko cyberprzestępczości.

3.2 Wniosek w sprawie agencji ENISA stanowi punkt odniesienia zarówno dla obowiązujących przepisów w dziedzinie polityki, jak i dla nowych inicjatyw przedstawionych w Europejskiej agendzie cyfrowej.

3.3 Istniejące polityki, które ma wspierać agencja ENISA, obejmują:

(i) europejskie forum państw członkowskich (ang. European Forum for Member States, EFMS), ukierunkowane na pobudzanie dyskusji i wymianę dobrych praktyk na rzecz ustalenia wspólnych celów politycznych i priorytetów w zakresie bezpieczeństwa i odporności infrastruktury TIK;

(ii) europejskie partnerstwo publiczno-prywatne na rzecz odporności (ang. European Public Private Partnership for Resilience, EP3R), które stanowi elastyczne ramy europejskie w zakresie zarządzania odpornością infrastruktury TIK i którego działalność polega na promowaniu współpracy między sektorem publicznym i sektorem prywatnym w zakresie kwestii dotyczących bezpieczeństwa i odporności;

(iii) program sztokholmski, przyjęty przez Radę Europejską w dniu 11 grudnia 2009 r., promujący polityki zapewniające bezpieczeństwo sieci i umożliwiające szybsze reagowanie na wypadek ataków cybernetycznych w Unii.

3.4 Nowe procesy, które ma wspierać agencja ENISA, są następujące:

(i) intensyfikacja działań w ramach EFMS,

(ii) wsparcie EP3R poprzez dyskusje poświęcone innowacyjnym środkom i instrumentom służącym poprawie bezpieczeństwa i odporności,

(iii) praktyczne wdrożenie wymogów bezpieczeństwa określonych w pakiecie regulacyjnym w sprawie łączności elektronicznej,

(iv) ułatwianie ogólnounijnych ćwiczeń w zakresie gotowości w dziedzinie bezpieczeństwa cybernetycznego,

(v) ustanowienie zespołu reagowania na incydenty komputerowe (CERT) dla instytucji UE,

(vi) mobilizowanie i wspieranie państw członkowskich w zakresie ustalania składu oraz, w razie konieczności, inicjowania działalności krajowych / rządowych CERT w celu ustanowienia dobrze funkcjonującej sieci CERT obejmującej całą Europę,

(vii) podnoszenie świadomości wyzwań związanych z bezpieczeństwem sieci i informacji.

3.5 Zanim ostatecznie opracowano wniosek, rozważono pięć różnych wariantów polityki. Z każdym z nich łączyły się warianty dotyczące zadań i zasobów. Wybrano wariant trzeci, który obejmuje rozszerzenie obecnie określonych zadań agencji ENISA oraz włączenie agencji odpowiedzialnych za egzekwowanie prawa i ochronę prywatności jako zainteresowanych stron.

3.6 Zgodnie z wariantem 3 zmodernizowana agencja bezpieczeństwa sieci i informacji wnosiłaby wkład w:

— zmniejszenie rozdrobnienia podejść krajowych (czynnik powodujący problemy nr 1), usprawnienie polityki i procesów decyzyjnych bazujących na danych i wiedzy / informacjach (czynnik powodujący problemy nr 3) oraz podnoszenie ogólnej świadomości zagrożeń i wyzwań związanych z bezpieczeństwem sieci i informacji i podejmowanie odpowiednich działań (czynnik powodujący problemy nr 4) poprzez wspieranie:

  — bardziej efektywnego gromadzenia przez każde państwo członkowskie istotnych informacji o ryzyku, zagrożeniach i sytuacjach podatności na zagrożenia,

  — większej dostępności informacji o obecnych i przyszłych wyzwaniach i zagrożeniach związanych z bezpieczeństwem sieci i informacji,

  — stanowienia lepszej jakościowo polityki bezpieczeństwa sieci i informacji w państwach członkowskich;

— poprawę zdolności Europy do wczesnego ostrzegania i reagowania (czynnik powodujący problemy nr 2) poprzez:

  — pomoc dla Komisji i państw członkowskich w organizacji ogólnoeuropejskich ćwiczeń, co pozwoli na osiągnięcie korzyści skali w reagowaniu na incydenty dotyczące całej UE,

  — ułatwienie funkcjonowania EP3R, co może ostatecznie prowadzić do dalszych inwestycji wynikających z celów wspólnej polityki i ogólnounijnych norm bezpieczeństwa i odporności;

— promowanie wspólnego globalnego podejścia do bezpieczeństwa sieci i informacji (czynnik powodujący problemy nr 5) poprzez:

  — intensyfikację wymiany informacji i wiedzy z krajami nienależącymi do UE;

— bardziej skuteczne i efektywne zwalczanie cyberprzestępczości (czynnik powodujący problemy nr 7) poprzez:

  — zaangażowanie w zadania nieoperacyjne związane z aspektami bezpieczeństwa sieci i informacji dotyczącymi egzekwowania prawa i współpracy sądowej, takie jak dwukierunkowa wymiana informacji i szkolenia (np. we współpracy z Europejskim Kolegium Policyjnym CEPOL).

3.7 Zgodnie z wariantem 3 agencja ENISA dysponowałaby wszystkimi zasobami niezbędnymi do prowadzenia działalności w zadowalający, efektywny sposób, tj. umożliwiający rzeczywiste oddziaływanie. Mając do dyspozycji większe zasoby ([5]), ENISA mogłaby odgrywać znacznie bardziej aktywną rolę i podejmować więcej inicjatyw mających na celu stymulowanie czynnego udziału zainteresowanych stron. Ponadto taka nowa sytuacja umożliwiałaby większą elastyczność pod względem szybkiego reagowania na zmiany w stale zmieniającym się środowisku bezpieczeństwa sieci i informacji.

3.8 Wariant polityki nr 4 obejmuje dodanie funkcji operacyjnych dotyczących zwalczania ataków cybernetycznych i reagowania na incydenty cybernetyczne. Oprócz działań określonych powyżej, agencja pełniłaby funkcje operacyjne, m.in. przyjmując bardziej aktywną rolę w ochronie krytycznej infrastruktury informatycznej UE, np. w zakresie zapobiegania incydentom i reagowania na nie, występując zwłaszcza w charakterze unijnego zespołu reagowania na incydenty komputerowe (CERT) w zakresie bezpieczeństwa sieci i informacji oraz koordynując działania krajowych zespołów CERT jako centrum kryzysowe UE ds. bezpieczeństwa sieci i informacji, włącznie z codziennym zarządzaniem działalnością i współpracą ze służbami ratunkowymi.

3.9 Wariant 4 miałby większe oddziaływanie na poziomie operacyjnym, wykraczające poza skutki wariantu 3. Występując w charakterze unijnego zespołu CERT ds. bezpieczeństwa sieci i informacji oraz koordynując działania krajowych zespołów CERT, agencja przyczyniłaby się np. do osiągania większych korzyści skali w zakresie reagowania na incydenty dotyczące całej UE i do obniżenia ryzyka operacyjnego ponoszonego przez przedsiębiorstwa dzięki wyższemu poziomowi bezpieczeństwa i odporności. Ten wariant wymaga znacznego zwiększenia budżetu i zasobów ludzkich agencji, co budzi obawy dotyczące jej zdolności absorpcyjnej i efektywnego wykorzystania budżetu w stosunku do uzyskanych korzyści.

3.10 Wariant polityki nr 5 obejmuje funkcje operacyjne w zakresie wspierania organów egzekwowania prawa i organów sądowych w zwalczaniu cyberprzestępczości. Oprócz działań wymienionych w wariancie 4, ten wariant umożliwiałby agencji:

— udzielanie wsparcia w zakresie prawa procesowego (por. konwencja o cyberprzestępczości): np. gromadzenie danych o ruchu w sieci, przechwytywanie danych dotyczących treści, monitorowanie przepływów w przypadku ataków typu denial-of-service;

— odgrywanie roli centrum wiedzy specjalistycznej na potrzeby dochodzeń obejmujących aspekty bezpieczeństwa sieci i informacji.

3.11 Dzięki dodaniu funkcji operacyjnych dotyczących wsparcia egzekwowania prawa i organów sądowych wariant 5 zapewniłby większą skuteczność zwalczania cyberprzestępczości niż warianty 3 i 4.

3.12 Wariant 5 wymagałby znacznego zwiększenia zasobów ludzkich agencji i ponownie budziłby obawy co do jej zdolności absorpcyjnej i efektywnego wykorzystania budżetu.

3.13 Podczas gdy zarówno wariant 4, jak i wariant 5 miałyby bardziej pozytywne skutki niż wariant 3, Komisja uważa, że istnieje kilka powodów, by nie realizować tych wariantów:

— warianty te stanowiłyby dla państw członkowskich rozwiązania wrażliwe politycznie, jeśli chodzi o obowiązki w zakresie ochrony krytycznej infrastruktury informacyjnej (tj. wiele państw członkowskich nie opowiedziałoby się za centralizacją funkcji operacyjnych);

— poszerzenie mandatu w sposób omówiony w związku z wariantami 4 i 5 może postawić agencję w dwuznacznej sytuacji;

— dodanie tych nowych i zupełnie różnych zadań operacyjnych do mandatu agencji może wiązać się z dużymi wyzwaniami w krótkiej perspektywie czasowej; istnieje też poważne ryzyko, że agencja nie uzyskałaby w rozsądnym przedziale czasu zdolności do należytego wykonywania takich zadań;

— wreszcie, koszt wdrożenia wariantów 4 i 5 jest zniechęcająco wysoki: wymagany budżet byłby cztero- lub pięciokrotnie większy od obecnego budżetu agencji ENISA.

([5]) Zachowanie wzmianki o większych zasobach zależy od tego, czy wniosek w sprawie agencji ENISA zostanie zatwierdzony w obecnej postaci.

4. **Przepisy rozporządzenia**

4.1 Agencja pomaga Komisji i państwom członkowskim w spełnianiu wymogów prawnych i regulacyjnych w zakresie bezpieczeństwa sieci i informacji.

4.2 Zarząd określa ogólny kierunek działalności agencji.

4.3 W skład zarządu wchodzi po jednym przedstawicielu każdego z państw członkowskich, trzech przedstawicieli wyznaczonych przez Komisję oraz po jednym przedstawicielu branży TIK, grup konsumenckich i ekspertów akademickich.

4.4 Agencją zarządza niezależny dyrektor wykonawczy, którego zadaniem będzie opracowanie programu pracy agencji i przedłożenie go zarządowi do zatwierdzenia.

4.5 Dyrektor wykonawczy odpowiada także za sporządzenie rocznego budżetu, który będzie wspierał realizację programu pracy. Zarząd powinien przedstawić zarówno budżet, jak i program pracy do zatwierdzenia przez Komisję i państwa członkowskie.

4.6 Na wniosek dyrektora wykonawczego zarząd ustanawia Stałą Grupę Przedstawicieli Zainteresowanych Stron złożoną z ekspertów reprezentujących branżę TIK, grupy konsumenckie, ekspertów akademickich, organy odpowiedzialne za egzekwowanie prawa i ochronę prywatności.

4.7 Zważywszy, że rozporządzenie jest wciąż na etapie wniosku, przedstawione liczby są niepewne. Obecnie w agencji zatrudnionych jest 44–50 pracowników i dysponuje ona budżetem wysokości 8 mln euro. Teoretycznie, realizacja wariantu 3 mogłaby pociągać za sobą zatrudnienie 99 pracowników i wymagać budżetu wysokości 17 mln euro.

4.8 W rozporządzeniu zaproponowano mandat na okres 5 lat.

Bruksela, 17 lutego 2011 r.

Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego
Staffan NILSSON