EUROPÄISCHE KOMMISSION

Brüssel, den 30.9.2010
SEK(2010) 1127

ARBEITSDOKUMENT DER KOMMISSIONSDIENSTSTELLEN

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

Begleitdokument zum

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die Europäische Agentur für Netz- und Informationssicherheit (ENISA)

{KOM(2010) 521 endgültig}
{SEK(2010) 1126}

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

1. GELTUNGSBEREICH UND KONTEXT

1.1. Geltungsbereich

Im Mittelpunkt dieser Folgenabschätzung steht die Frage, wie eine modernisierte Agentur für Netz- und Informationssicherheit (NIS), die als geeignetes und notwendiges Politikinstrument für den Umgang mit NIS-Herausforderungen breite Anerkennung findet, am besten gestaltet werden sollte, damit sie die Einrichtungen der Mitgliedstaaten und die Kommission bei der Erreichung ihrer Ziele im Bereich der NIS-Politik unterstützen kann, wenn das Mandat der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) im März 2012 ausläuft.

1.2. Kontext

In der heutigen Welt hängen Wirtschaft und Gesellschaft entscheidend davon ab, dass Informations- und Kommunikationstechnologien (IKT) ordnungsgemäß funktionieren. Deshalb ist es von überragender Bedeutung sicherzustellen, dass die Systeme stabil laufen und dass die Nutzer ihnen vertrauen. Die zunehmende Anzahl von Bedrohungen, Angriffen und Schadprogrammen gegen diese Systeme könnte eine Gefahr für das ordnungsgemäße Funktionieren grundlegender Netz- und Informationsinfrastrukturen darstellen. Da diese Systeme und Netze länderübergreifend arbeiten, ist auf die Herausforderung der Netz- und Informationssicherheit (NIS) eine europäische Antwort notwendig.

Zur Bewältigung dieser Fragen wurde die Europäische Agentur für Netz- und Informationssicherheit (ENISA) 2004 für einen Zeitraum von fünf Jahren gegründet[1]. Das Hauptziel war die *„Gewährleistung einer hohen und effektiven Netz- und Informationssicherheit innerhalb der Gemeinschaft und der Entwicklung einer Kultur der Netz- und Informationssicherheit, die Bürgern, Verbrauchern, Unternehmen und Organisationen des öffentlichen Sektors der Europäischen Union Nutzen bringt und damit zum reibungslosen Funktionieren des Binnenmarktes beiträgt“*.

Seitdem haben sich die NIS-Herausforderungen mit der Technologie- und Marktentwicklung ständig verändert. Deshalb leitete die Kommission schon lange vor dem Auslaufen der ENISA-Verordnung im März 2009 einen Prozess ein, um gemeinsam mit den einschlägigen Akteuren jene Politikvorschläge zu bestimmen, die den NIS-Zielen der EU ab 2009 am besten dienen. Nach einer Halbzeitbewertung[2] der ENISA 2007 und einer öffentlichen Konsultation[3] erließen der Rat und das Europäische Parlament am 24. September 2008 eine Verordnung zur Verlängerung des bisherigen ENISA-Mandats um drei Jahre bis zum 13. März 2012[4]. In den Erwägungsgründen dieser Verordnung riefen der Rat und das Europäische Parlament dazu

---

1 Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit.

2 Mitteilung der Kommission an das Europäische Parlament und den Rat über die Bewertung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA), KOM(2007) 285 endg. vom 1.6.2007: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:DE:NOT.

3 Die Konsultation lief vom 13. Juni bis zum 7. September 2007.

4 Verordnung (EG) Nr. 1007/2008 des Europäischen Parlaments und des Rates vom 24. September 2008 zur Änderung der Verordnung (EG) Nr. 460/2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit bezüglich deren Bestehensdauer, ABl. L 293 vom 31.10.2008.

auf, *„**weitergehende Überlegungen über die Zukunft der ENISA und die allgemeine Ausrichtung der europäischen Bemühungen um eine verbesserte Netz- und Informationssicherheit**“* anzustellen.

Die Kommission förderte die Diskussion im November 2008 durch die Einleitung einer weiteren EU-weiten öffentlichen Konsultation über die möglichen Ziele einer verstärkten Politik für Netz- und Informationssicherheit und die Mittel und Wege, um diese Ziele zu erreichen[5]. Darüber hinaus veranstaltete die Kommission im Dezember 2008 einen Workshop mit NIS-Experten der zuständigen Stellen in den Mitgliedstaaten über die Instrumente und Verfahren einer verstärkten Politik für Netz- und Informationssicherheit. Ferner nahm die Kommission im März 2009 eine Mitteilung über den Schutz kritischer Informationsinfrastrukturen[6] (CIIP) an, in der sie der ENISA eine Schlüsselrolle zuweist, wenn es darum geht, die EU bei der Stärkung der Sicherheit, Abwehrbereitschaft und Stabilität zu unterstützen. Dieser Ansatz wurde auf der Ministerkonferenz über den Schutz kritischer Informationsinfrastrukturen (CIIP) am 27. und 28. April in Tallinn gebilligt, in deren Schlussfolgerungen es hieß: ***„Die neuen und lang andauernden künftigen Herausforderungen erfordern ein gründliches Überdenken und Überarbeiten des Mandats der Agentur, die es dieser gestatteten, sich besser auf die EU-Prioritäten und -Erfordernisse zu konzentrieren**, eine flexiblere Reaktionsfähigkeit zu erzielen, europäische Fertigkeiten und Kompetenzen zu entwickeln und die operative Effizienz und die Gesamtwirkung der Agentur zu fördern. Auf diese Weise könnte ENISA auf Dauer zu einem Trumpf für alle Mitgliedstaaten und die Europäische Union insgesamt werden.“*

Am 18. Dezember 2009 verabschiedete der Rat eine Entschließung über *„ein kooperatives europäisches Vorgehen im Bereich der Netz- und Informationssicherheit“*[7], in der betont wird: *„**Die ENISA sollte im Rahmen eines überarbeiteten Mandats als Kompetenzzentrum der Europäischen Union für EU-bezogene Netz- und Informationssicherheit dienen.**“*

In der Kommissionsstrategie „Europa 2020“ für intelligentes, nachhaltiges und integratives Wachstum[8] wird als eine der sieben Leitinitiativen zu deren Umsetzung die Digitale Agenda für Europa genannt, in der die NIS eine zentrale Rolle spielt. **Ziel dieser Politikinitiative für Vertrauen und Sicherheit in der Digitalen Agenda für Europa ist es, die EU, die Mitgliedstaaten und die Akteure in die Lage zu versetzen, ein hohes Niveau an Reaktionsfähigkeit und Abwehrbereitschaft aufzubauen, um NIS-Probleme zu verhüten, zu erkennen und besser bewältigen zu können**. Dies wird zu mehr Vertrauen und Sicherheit im europäischen digitalen Binnenmarkt beitragen und die Wettbewerbsfähigkeit der europäischen Unternehmen verbessern.

---

5 Vom 7. November 2008 bis 9. Januar 2009, Bericht abrufbar unter http://ec.europa.eu/information_society/policy/nis/nis_public_consultation/index_en.htm.

6 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen, KOM(2009) 149 vom 30.3.2009.

7 Entschließung des Rates vom 18. Dezember 2009 über ein kooperatives europäisches Vorgehen im Bereich der Netz- und Informationssicherheit (NIS) (ABl. C 321 vom 29.12.2009, S. 1).

8 KOM(2010) 2020.

2. PROBLEMSTELLUNG

2.1. Worin besteht das Problem?

Ermittelt wurden folgende Problempunkte, die die Akteure für NIS-Bedrohungen und NIS-Störungen anfällig machen. Sie alle belegen die Notwendigkeit einer verlässlichen Struktur auf EU-Ebene, die das Problem angehen und überall in Europa mit den sich ständig ändernden Technologie- und Marktbedingungen im Bereich der NIS Schritt halten kann.

- **Die Vielfalt und Uneinheitlichkeit nationaler Konzepte.** NIS-Probleme richten sich nicht nach nationalen Grenzen und können deshalb nicht ausschließlich auf nationaler Ebene wirksam gelöst werden. Gleichzeitig gibt es große Unterschiede in der Art und Weise, wie die Behörden in verschiedenen Mitgliedstaaten mit diesen Problemen umgehen. Die Vielzahl der unterschiedlichen Sicherheitsanforderungen in verschiedenen Mitgliedstaaten bedeutet eine Kostenbelastung für EU-weit tätige Unternehmen und führt zu einer Fragmentierung und einem Verlust an Wettbewerbsfähigkeit im europäischen Binnenmarkt.

- **Beschränkte Frühwarn- und Reaktionsfähigkeit bei Störungen in Europa.** Die derzeitigen, nationalen Frühwarn- und Krisenbewältigungssysteme weisen erhebliche Unterschiede zwischen den Mitgliedstaaten auf, wogegen es ein EU-System nicht gibt. Es besteht daher ein Bedarf an EU-Politikinstrumenten für die Ermittlung von NIS-Risiken und -Anfälligkeiten, für die Schaffung geeigneter Reaktionsmechanismen und für die Sicherstellung, dass den Beteiligten diese Reaktionsmechanismen bekannt sind und von ihnen auch angewandt werden.

- **Ein Mangel an zuverlässigen Daten und unzureichende Kenntnis über sich verändernde Probleme.** Es liegen kaum verlässliche quantitative Informationen über die Folgen oder auch nur das Auftreten von NIS-Störungen vor, weshalb es für politische Entscheidungsträger schwierig ist, angemessene politische Maßnahmen zu ergreifen, und für Unternehmen schwierig ist, über Investitionen im Bereich der Sicherheit zu entscheiden.

- **Geringes Bewusstsein für Risiken und Herausforderungen im Bereich der NIS.** Die Verantwortung für die Gewährleistung der Netz- und Informationssicherheit liegt bei den einzelnen Akteuren, ihre Verantwortlichkeiten werden jedoch nicht immer eindeutig festgelegt und mitgeteilt. Einerseits neigen die Verbraucher zu einer Unterschätzung der NIS-Risiken und sind sich ihrer eigenen Verantwortung für die Sicherung ihrer IKT-Systeme nicht bewusst. Andererseits sehen die Unternehmen häufig vor allem die Kosten der NIS, nicht aber die mit ihr verbundenen potenziellen Einsparungen.

- **Die internationale Dimension der Probleme im Bereich der Netz- und Informationssicherheit.** NIS-Bedrohungen und daran anschließende Störungen sind von Natur aus international, so dass EU-Maßnahmen weniger wirksam sein können, wenn NIS-Problemen nicht auch auf internationaler Ebene in angemessener Weise begegnet wird. Daher muss eine EU-Strategie und eine Bezugsstelle für NIS geschaffen werden, um die internationale Position der EU zu stärken.

- **Die Notwendigkeit von Kooperationsmodellen für die angemessene Umsetzung der Politik.** Für eine angemessene Umsetzung der NIS-Politik werden Kooperationsmodelle auf EU-Ebene benötigt. Die Akteure brauchen Orientierungen für die Feststellung von

NIS-Bedrohungen und die Entwicklung einer guten Praxis für die Umsetzung bestehender NIS-Vorgaben.

- **Die Notwendigkeit eines effizienteren Vorgehens gegen Cyberkriminalität.** Bemühungen zur Erhöhung der Netz- und Informationssicherheit wurden bislang überwiegend im Rahmen der bisherigen ersten Säule organisiert, d. h. die Fragen wurden zwischen den Organen erörtert. Mit dem Inkrafttreten des Vertrags von Lissabon ist nun jedoch eine breitere Palette von Aufgaben für eine NIS-Agentur in Betracht zu ziehen, die auch Gebiete der „zweiten und dritten Säule" betreffen, d. h. Angelegenheiten, in denen der Rat bisher allein entschied.

2.2. Wen betrifft das Problem am meisten?

Störungen der Netz- und Informationssicherheit haben sehr große Auswirkungen auf eine Vielzahl von Beteiligten, zu denen große und kleine Unternehmen, öffentliche Stellen und Verwaltungen, aber auch einzelne Bürger zählen. Mit anderen Worten, wir sind alle von der NIS betroffen und für sie verantwortlich.

Über die genaue Zahl der NIS-Störungen oder ihre wirtschaftlichen Folgen gibt es keine oder nur wenige objektive quantitative Informationen. Einen Anhaltspunkt liefert die IDC-EMEA-Marktuntersuchung[9], der zufolge 28 % der Privathaushalte in der EU-27 in den letzten 12 Monaten von Spam- oder Virenproblemen betroffen waren. Im Durchschnitt waren etwa 7 % der Geschäftsnutzer im letzten Jahr mit einem Sicherheitsproblem konfrontiert.

3. GRÜNDE FÜR EU-MAßNAHMEN, MEHRWERT AUF EU-EBENE UND SUBSIDIARITÄT

Wegen der wechselseitigen Abhängigkeit der Netze und Informationssysteme ist es für einen einzelnen Beteiligten extrem schwierig oder sogar unmöglich, die globalen wirtschaftlichen und gesellschaftlichen Folgen seiner Maßnahmen zum Schutz vor NIS-Störungen richtig einzuschätzen. Eine unterschiedliche Politik und Praxis auf nationaler Ebene stört den Binnenmarkt, sowohl wegen der negativen Auswirkungen von NIS-Störungen (unzureichende Maßnahmen beeinträchtigen die Märkte in anderen Mitgliedstaaten) als auch der positiven Auswirkungen einer guten NIS-Praxis (die gute Praxis in einem Mitgliedstaat verbessert die NIS insgesamt und bildet somit ein eindeutiges gesellschaftlichen Gut). Ein politisches Eingreifen der EU ist daher gerechtfertigt, denn es würde einen echten Mehrwert für das Funktionieren des Binnenmarktes bedeuten. Ein solcher Mehrwert wurde auch in der Verordnung (EG) Nr. 460/2004 zur Errichtung der ENISA anerkannt, die festlegt, dass die ENISA mit ihren Zuständigkeiten einen Beitrag zum reibungslosen Funktionieren des Binnenmarktes leisten soll.

Darüber hinaus ist ein Eingreifen der EU im Bereich der NIS-Politik auch durch das *Subsidiaritätsprinzip* gerechtfertigt. Wie schon in der Mitteilung über den Schutz kritischer Informationsinfrastrukturen dargelegt, liefe eine EU-Strategie des Nichteingreifens in die nationale NIS-Politik eher darauf hinaus, dass die Mitgliedstaaten trotz der wechselseitigen Abhängigkeit der Informationssysteme aufgefordert würden, lediglich ihren eigenen

---

[9] IDC EMEA, *The European Network and Information Security Market, Scenario, Trends and Challenges* (Der europäische Markt der Netz- und Informationssicherheit – Szenario, Trends, Herausforderungen), April 2009, in Bezug auf die Eurobarometer-Erhebung zur elektronischen Kommunikation, April 2007.

Hinterhof zu bewachen. Ein hinreichendes Maß an Koordinierung zwischen den Mitgliedstaaten, das einen angemessenen Umgang mit den grenzübergreifenden Aspekten der NIS-Risiken sicherstellt, ist daher mit dem Subsidiaritätsprinzip vereinbar. Zudem würde eine EU-Maßnahme die Wirksamkeit etwaiger nationaler Strategien erhöhen.

Die EU-Bürger vertrauen in zunehmendem Maße ihre Daten komplexen Informationssystemen an (z. B. beim *Cloud Computing*). Deshalb wird sich eine abgestimmte und kooperative NIS-Politik äußerst positiv auf den wirksamen *Schutz der Grundrechte* auswirken, insbesondere des Rechts auf den *Schutz der personenbezogenen Daten und der Privatsphäre*. Auch aus diesem Grund erscheinen EU-politische Maßnahmen hinlänglich gerechtfertigt.

4. POLITISCHE ZIELE

In dieser Folgenabschätzung wird geprüft, wie eine modernisierte NIS-Agentur, die als die am besten geeignete Organisationsstruktur breite Anerkennung findet, am besten gestaltet werden sollte, damit sie im Zusammenspiel mit anderen EU-Instrumenten zur Erreichung der politischen Ziele beitragen kann.

Das allgemeine Ziel besteht darin, die EU, die Mitgliedstaaten und die Akteure in die Lage zu versetzen, ein hohes Niveau an Reaktionsfähigkeit und Abwehrbereitschaft aufzubauen, um NIS-Probleme zu verhüten, zu erkennen und besser zu bewältigen. Dies wird zu mehr Vertrauen und Sicherheit im europäischen digitalen Binnenmarkt beitragen und die Wettbewerbsfähigkeit der europäischen Unternehmen verbessern.

Dieses Gesamtziel gliedert sich in **sieben Einzelziele**:

(1) **Angleichung der Regulierungskonzepte** – Orientierungshilfen und Beratung für die Kommission und die Mitgliedstaaten bei der Aktualisierung und Weiterentwicklung eines ganzheitlichen Regelungsrahmens auf dem Gebiet der Netz- und Informationssicherheit;

(2) **Verhütung, Erkennung und Bewältigung** – Verbesserung der Abwehrbereitschaft durch einen Beitrag zu einer europäischen Frühwarn- und Reaktionsfähigkeit sowie europaweiten Notfallplänen und Übungen;

(3) **Unterstützung politischer Entscheidungsprozesse** – Hilfestellung und Beratung für die Kommission und die Mitgliedstaaten;

(4) **Stärkung der Eigenverantwortung der Akteure** – Entwicklung einer Kultur des Sicherheits- und Risikomanagements durch die Förderung des Informationsaustauschs und einer breiten Zusammenarbeit zwischen Akteuren aus dem öffentlichen und privaten Sektor, auch zum unmittelbaren Nutzen der Bürger und KMU, sowie durch die Entwicklung einer Kultur des Problembewusstseins im Bereich der NIS;

(5) **Stärkung der Rolle Europas als international ernstzunehmender Partner** – Aufbau einer hochrangigen Zusammenarbeit mit Drittländern und internationalen Organisationen, um auf ein gemeinsames globales NIS-Konzept hinzuwirken und Impulse für hochrangige internationale Initiativen in Europa zu geben;

(6) **Kooperative Umsetzung** – Förderung der Zusammenarbeit bei der Umsetzung der NIS-Politik;

(7) **Bekämpfung der Cyberkriminalität** – Entwicklung wirksamer Antworten für die NIS-Aspekte der Cyberkriminalität durch die Zusammenarbeit mit den Behörden der (früheren) zweiten und dritten Säule, z. B. mit Europol.

5. MÖGLICHE ORGANISATIONSFORMEN UND POLITIKOPTIONEN

In der Folgenabschätzung (Kapitel 4 und Anhang 4) wird eine Reihe möglicher Organisationsformen für die Umsetzung der oben genannten Politikoptionen geprüft: i) eine Agentur, ii) eine mehr oder weniger förmliche öffentlich-private Partnerschaft (ÖPP), iii) ein informelles Kontaktnetz, iv) ein ständiges Netz der zuständigen Stellen und v) direkte Eingliederung in eine Kommissionsdienststelle.

Im Vergleich dieser unterschiedlichen Organisationsformen erscheint die Agentur als das am besten geeignete Politikinstrument, weil sie folgende Vorteile aufweist: 1) Rechtssicherheit sowohl in Bezug auf die Organisationsstruktur als auch die inhaltlichen Aspekte, 2) ihre Eignung für die besonderen Belange eines so sensiblen Sektors wie der NIS (Stelle mit externer Sachkenntnis, Koordinierung der Beziehungen mit den Akteuren, Einbeziehung/Mitarbeit der Mitgliedstaaten) und 3) Anerkennung und Ruf der ENISA in NIS-Kreisen.

Folglich wurden die folgenden Politikoptionen für die Organisationsform einer Agentur ausgearbeitet und ausführlich bewertet.

Politikoption 1: Keine Maßnahmen

Bei der Option „Keine Maßnahmen“ wird davon ausgegangen, dass die ENISA ab März 2012 nicht mehr besteht und die laufenden ENISA-Tätigkeiten auch von keiner anderen EU-Einrichtung übernommen werden.

Eine Schließung der ENISA würde bedeuten, dass alle bisherigen Investitionen, z. B. in den Aufbau einer Organisation, die für hochspezialisierte Fachleute attraktiv ist, in den Aufbau eines Erfahrungsschatzes und in die Vernetzung von und mit Akteuren und internationalen Einrichtungen, gerade in dem Moment abgezogen würden, in dem die bestehende Agentur ihre volle Arbeitsfähigkeit erreicht hat.

Die komplexe Natur der NIS-Problematik in ganz Europa erfordert eine modernisierte und gestärkte Agentur, nicht die Schließung der bestehenden Agentur. Bekräftigt wird dies auch durch die Rolle, die z. B. der reformierte Rechtsrahmen für die elektronische Kommunikation[10] der ENISA ausdrücklich zuweist, und durch die von den Akteuren allgemein geäußerte Unterstützung für eine größere Rolle einer europäischen NIS-Agentur.

Politikoption 2: Unveränderte Fortführung der gegenwärtigen Maßnahmen

Option 2 ist das „Weiter-wie-bisher“-Szenario, d. h. die Fortführung des gleichen Politikinstruments in identischer Form und mit gleicher Mittelausstattung. Die Akteure sind sich im Allgemeinen darin einig, dass die ENISA inzwischen zu einer glaubwürdigen Bezugsstelle für NIS-Fragen gereift ist und sich in ihrem Fachgebiet zu einem Exzellenzzentrum entwickelt hat.

---

[10] Siehe http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2009:337:SOM:DE:HTML.

Mit ihrer derzeitigen Personalausstattung und angesichts der Haushaltsbeschränkungen wird die Agentur ihren Einfluss aber nur in einer sehr begrenzten Zahl von NIS-Fragen ausüben können. Dies steht im krassen Widerspruch zu den Gesamterwartungen der Akteure an die Agentur und dürfte letztlich zu einer Vertrauenskrise führen, wenn der Agentur nicht die Möglichkeit gegeben wird, sich weiterzuentwickeln und diesen wachsenden Erwartungen gerecht zu werden.

Politikoption 3: Ausweitung der gegenwärtigen ENISA-Funktionen und Einbindung der Strafverfolgungs- und Datenschutzbehörden als vollwertige Akteure

In dieser Option wird die Rolle eine NIS-Agentur erweitert und auf folgende Aufgaben ausgerichtet:

- Aufbau und Pflege eines Verbindungsnetzes zwischen den Akteuren sowie eines Wissensnetzes;
- Funktion als NIS-Unterstützungszentrum für die Politikgestaltung und -umsetzung (insbesondere was den Schutz der Privatsphäre, elektronische Signaturen, elektronische Identitäten (eID) und NIS-Standards bei öffentlichen Aufträgen anbelangt);
- Unterstützung der EU-Politik für den Schutz kritischer Informationsinfrastrukturen (CIIP) und deren Widerstandsfähigkeit (Übungen, EP3R[11], Europäisches Informations- und Warnsystem usw.);
- Schaffung eines EU-Rahmens für die Sammlung von NIS-Daten, einschließlich der Entwicklung von Methoden und Vorgehensweisen für die gesetzliche Erfassung und den Austausch solcher Daten;
- Untersuchungen und Berichterstattung über die wirtschaftlichen Aspekte der NIS;
- Förderung der Zusammenarbeit mit Drittländern und internationalen Organisationen, um auf ein gemeinsames globales NIS-Konzept hinzuwirken und Impulse für hochrangige internationale Initiativen in Europa zu geben;
- Durchführung nichtoperativer Maßnahmen im Zusammenhang mit den NIS-Aspekten der Strafverfolgung und justiziellen Zusammenarbeit.

Die Agentur würde über alle notwendigen Ressourcen verfügen, damit sie ihre Aufgaben zufriedenstellend und gründlich wahrnehmen und dadurch eine tatsächliche Wirkung erzielen kann. Mit einer aufgestockten Mittelausstattung könnte die ENISA deutlich proaktiver werden und mehr Initiativen zur Förderung der aktiven Mitarbeit der Akteure ergreifen. Außerdem würde diese neue Situation mehr Flexibilität ermöglichen, so dass schnell auf Änderungen im sich ständig weiterentwickelnden NIS-Umfeld reagiert werden könnte.

Politikoption 4: Schaffung zusätzlicher operativer Funktionen zur Bekämpfung von Cyberangriffen und zur Reaktion auf Netzstörungen

Zusätzlich zu den in Option 3 dargelegten Tätigkeiten würde die Agentur operative Funktionen übernehmen, z. B. eine aktivere Rolle beim Schutz kritischer Infrastrukturen in der EU, etwa bei der Verhütung und Bewältigung von Störungen, indem sie insbesondere als IT-Notfallteam (*Computer Emergency Response Team*, CERT) der EU im NIS-Bereich wirkt

[11] *European Public Private Partnership for Resilience* (Europäische öffentlich-private Partnerschaft für Robustheit), siehe KOM(2009) 149.

und als EU-NIS-Krisenzentrum die nationalen CERTs sowohl im Tagesgeschäft als auch bei Notfällen koordiniert.

Diese Option würde eine beträchtliche Aufstockung der finanziellen und personellen Mittel der Agentur erforderlich machen, was Bedenken bezüglich ihrer Aufnahmefähigkeit und der effektiven Mittelverwendung im Verhältnis zu den angestrebten Zielen hervorruft.

Politikoption 5: Schaffung zusätzlicher operativer Funktionen zur Unterstützung der Strafverfolgungs- und der Justizbehörden bei der Bekämpfung von Cyberkriminalität

Zusätzlich zu den in Option 4 dargelegten Tätigkeiten würde diese Option für die Agentur folgende Funktionen vorsehen:

- Unterstützung in verfahrensrechtlichen Fragen (vgl. das Übereinkommen über Computerkriminalität): z. B. Sammeln von Verkehrsdaten, Abfangen von Inhaltsdaten, Überwachung von Datenströmen im Fall von DoS-Überlastungsangriffen (Denial-of-Service-Angriffen);
- Wirken als Kompetenzzentrum für die Untersuchung von Straftaten und deren NIS-Aspekte.

Wie bei Option 4 würde dies eine beträchtliche Aufstockung des Haushalts der Agentur erforderlich machen, was auf ähnliche Bedenken bezüglich ihrer Aufnahmefähigkeit und der effektiven Mittelverwendung stößt.

6. VERGLEICH DER POLITIKOPTIONEN UND ABSCHÄTZUNG DER FOLGEN

Aus der Analyse der möglichen wirtschaftlichen, sozialen und umweltpolitischen Folgen ergibt sich, dass die ***Option 1*** sich in jeder Hinsicht negativ auswirken und die Lage verschlechtern würde.

Die ***Option 2*** erweist sich als suboptimal, weil der Agentur nicht die notwendigen Mittel zur Verfügung stünden, um den Herausforderungen der sich ständig verändernden NIS-Landschaft angemessen zu begegnen, was ihrem Ansehen schaden und letztlich in eine Vertrauenskrise führen könnte.

In ***Option 3*** würde eine modernisierte NIS-Agentur zu Folgendem beitragen:

Vereinheitlichung der nationalen Konzepte (Problempunkt 1), Stärkung einer daten- bzw. wissens-/informationsgestützten Politikgestaltung und Entscheidungsfindung (Problempunkt 3) und Stärkung des Bewusstseins für Risiken und Herausforderungen im Bereich der NIS und deren Bewältigung (Problempunkt 4) durch:

- eine effizientere Sammlung einschlägiger Informationen über Risken, Bedrohungen und Anfälligkeiten durch jeden einzelnen Mitgliedstaat;
- eine bessere Verfügbarkeit von Informationen über gegenwärtige und künftige Herausforderungen und Risiken im Bereich der NIS;
- eine höhere Qualität der NIS-Vorgaben in den Mitgliedstaaten.

Verbesserung der Frühwarn- und Reaktionsfähigkeit in Europa (Problempunkt 2) durch:

- Unterstützung der Kommission und der Mitgliedstaaten bei der Vorbereitung europaweiter Übungen, wodurch Größeneinsparungen bei der Bewältigung EU-weiter Störungen erzielt werden;

- die Förderung der Arbeit der EP3R, die dank gemeinsamer politischer Ziele und EU-weiter Normen für die Sicherheit und Widerstandfähigkeit letztlich zu mehr Investitionen führen könnte.

Förderung eines gemeinsamen globalen NIS-Konzepts (Problempunkt 5) durch:

- die Verbesserung des Informations- und Wissensaustauschs mit Nicht-EU-Ländern.

Effizientere und wirksamere Bekämpfung der Cyberkriminalität (Problempunkt 7) durch:

- Einbindung in nichtoperative Aufgaben im Zusammenhang mit den NIS-Aspekten der Strafverfolgung und justiziellen Zusammenarbeit, z. B. in den gegenseitigen Informationsaustausch und die Fortbildung (z. B. in Zusammenarbeit mit der Europäischen Polizeiakademie (EPA).

Option 4 würde eine größere Wirkung auf operativer Ebene zusätzlich zu der von Option 3 erzielen. Als EU-NIS-CERT und durch die Koordinierung der nationalen CERTs würde die Agentur zu höheren Größeneinsparungen bei der Bewältigung EU-weiter Störungen und zu geringeren operativen Risiken für Unternehmen beitragen, z. B. dank höherer Sicherheit und Widerstandsfähigkeit.

Option 5 würde durch zusätzliche operative Funktionen zur Unterstützung der Strafverfolgungs- und der Justizbehörden eine größere Wirkung bei der Bekämpfung der Cyberkriminalität erzielen als die Optionen 3 und 4.

Die Optionen 4 und 5 hätten zwar eine größere positive Wirkung als Option 3, sind aber beide für die Mitgliedstaaten politisch problematisch im Bezug auf deren Zuständigkeiten für den Schutz kritischer Informationsinfrastrukturen (eine Reihe von Mitgliedstaaten würde einer Zentralisierung operativer Funktionen nicht zustimmen). Außerdem könnte die Erweiterung des Mandats, wie in Option 4 und 5 geprüft, zu einer unklaren Stellung der Agentur führen. Überdies könnte sich die Aufnahme dieser neuen und völlig andersartigen operativen Aufgaben in das Mandat der Agentur kurzfristig als sehr schwierig erweisen, und es besteht die Gefahr, dass die Agentur nicht in der Lage ist, solche Aufgaben in einem vernünftigen zeitlichen Rahmen ordnungsgemäß zu erfüllen. Nicht zuletzt sind auch die Kosten der Umsetzung der Optionen 4 und 5 prohibitiv hoch – die dafür erforderlichen Haushaltsmittel beliefen sich auf das vier- bis fünffache des gegenwärtigen ENISA-Haushalts.

Im Vergleich der Folgen aller fünf Politikoptionen für die Organisationsform einer modernisierten NIS-Agentur scheiden die Optionen 1 und 2 aus, weil sie beide keine angemessene Bewältigung der komplexen NIS-Problematik auf EU-Ebene ermöglichen. Die Optionen 3, 4 und 5 würden dagegen die EU in die Lage versetzen, künftigen Fragen der NIS-Politik angemessen zu begegnen. Die Optionen 4 und 5 erscheinen zum gegenwärtigen Zeitpunkt allerdings als zu ehrgeizig, sowohl im Hinblick auf die politische Sensibilität der meisten Mitgliedstaaten als auch die damit verbundenen Haushaltsauswirkungen. Folglich ***ist die Option 3 am besten geeignet, um die sieben ermittelten NIS-Probleme am effizientesten zu bewältigen***.

7. ÜBERWACHUNG UND BEWERTUNG: WIE KÖNNEN TATSÄCHLICHE KOSTEN UND VORTEILE SOWIE DIE ERREICHUNG DER GEWÜNSCHTEN WIRKUNGEN GEMESSEN WERDEN?

Diese politische Initiative würde regelmäßige Bewertungen vorsehen, die von der Kommission dem Europäischen Parlament und dem Rat zugeleitet und der Öffentlichkeit zugänglich gemacht werden. Diese Bewertungen würden auch den Ansichten aller einschlägigen Beteiligten gemäß den mit dem Verwaltungsrat der Agentur vereinbarten Vorgaben Rechnung tragen, die Effektivität der Agentur bei der Erreichung ihrer Ziele beurteilen sowie abschätzen, ob eine Agentur noch immer ein wirksames Instrument ist und ob das Mandat der Agentur oder bestimmte Aspekte ihrer Gründungsverordnung geändert werden sollten. Im Anschluss an eine Bewertung würde der Verwaltungsrat der Agentur Empfehlungen für zweckmäßige Änderungen der Gründungsverordnung an die Kommission richten. Der Verwaltungsrat und der Direktor der Agentur sollten den Ergebnissen der Bewertungen bei der mehrjährigen Planung der Arbeit der Agentur Rechnung tragen.

Die Tätigkeit der Agentur unterliegt der Aufsicht des Bürgerbeauftragten gemäß Artikel 228 AEUV.