COMMISSIONE EUROPEA

Bruxelles, 30.9.2010
SEC(2010) 1127

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA VALUTAZIONE D'IMPATTO

Documento di accompagnamento alla

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo all'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)

{COM(2010) 521 definitivo}
{SEC(2010) 1126}

SINTESI DELLA VALUTAZIONE D'IMPATTO

1. CAMPO DI APPLICAZIONE E CONTESTO

1.1. Campo di applicazione

La presente valutazione di impatto ha lo scopo di determinare in che modo dovrebbe essere strutturata un'agenzia modernizzata responsabile della sicurezza delle reti e dell'informazione, ampiamente riconosciuta come strumento necessario e appropriato per far fronte alle difficoltà del settore, per aiutare gli Stati membri e la Commissione a raggiungere gli obiettivi della relativa strategia una volta scaduto il mandato dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), a marzo 2012.

1.2. Contesto

Al giorno d'oggi la società e l'economia fanno grande affidamento sul buon funzionamento delle tecnologie dell'informazione e della comunicazione (TIC), perciò è di grande importanza assicurare che i sistemi siano stabili e che gli utenti li usino con fiducia. Il numero crescente di minacce, attacchi e software maligni (*malware*) contro questi sistemi potrebbe mettere a rischio il funzionamento delle reti e delle infrastrutture informatiche di base. Dato il carattere transnazionale di tali sistemi e reti, occorre reagire alle sfide in materia di sicurezza delle reti e dell'informazione a livello europeo.

Per affrontare queste problematiche, nel marzo 2004[1] è stata istituita l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) per un periodo iniziale di cinque anni, al fine di "*assicurare un alto ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito [dell'Unione] e sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico dell'Unione europea, contribuendo in tal modo al buon funzionamento del mercato interno*".

Da allora, le sfide sono mutate con l'evolvere della tecnologia e del mercato, per questo motivo la Commissione, con largo anticipo rispetto alla scadenza del regolamento ENISA (marzo 2009) e coadiuvata dalle parti interessate, ha avviato una procedura per individuare le opzioni strategiche che potrebbero contribuire a raggiungere gli obiettivi in materia di sicurezza delle reti e dell'informazione dopo il 2009. Dopo una valutazione intermedia dell'ENISA (2007)[2] e una consultazione pubblica[3], il 24 settembre 2008 il Consiglio e Parlamento europeo hanno adottato un regolamento che prolunga di tre anni, fino al 13 marzo 2012, il mandato dell'ENISA nella sua forma iniziale[4]. Nei considerando a tale regolamento il Consiglio e il Parlamento europeo hanno invitato ad "***un'ulteriore riflessione***

---

1 Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.

2 Comunicazione della Commissione al Parlamento europeo e al Consiglio sulla valutazione dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) – COM(2007) 285 dell'1.6.2007. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:IT:NOT.

3 La consultazione pubblica si è svolta dal 13 giugno al 7 settembre 2007.

4 Regolamento (CE) n. 1007/2008 del Parlamento europeo e del Consiglio, del 24 settembre 2008, che modifica il regolamento (CE) n. 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione per quanto riguarda la durata dell'Agenzia (GU L 293 del 31.10.2008).

sull'orientamento generale degli sforzi europei volti ad aumentare la sicurezza delle reti e dell'informazione".

La Commissione ha facilitato la discussione lanciando, a novembre 2008, un'ulteriore consultazione pubblica a livello europeo sui possibili obiettivi di una strategia rafforzata in materia di sicurezza delle reti e dell'informazione e sulle modalità per raggiungere tali obiettivi[5]. A dicembre 2008 la Commissione ha organizzato un seminario incentrato sugli strumenti e i meccanismi necessari per consolidare la politica europea in materia di sicurezza delle reti e dell'informazione, al quale hanno partecipato esperti del settore provenienti dagli enti competenti degli Stati membri. Infine, a marzo 2009 la Commissione ha adottato una comunicazione sulla protezione delle infrastrutture critiche informatizzate (CIIP, *Critical Information Infrastructure Protection*)[6] che prevede, per l'ENISA, un ruolo centrale a supporto agli Stati membri per potenziare sicurezza, resilienza e preparazione. Questo approccio ha trovato largo appoggio in occasione della conferenza ministeriale dell'UE sulla protezione delle infrastrutture critiche informatizzate, tenutasi a Tallinn (Estonia) il 27 e 28 aprile 2009; una delle conclusioni raggiunte durante la conferenza è che "***le sfide nuove e durature che abbiamo davanti richiedono che il mandato dell'Agenzia venga profondamente ripensato e riformulato per incentrare maggiormente l'attenzione sulle priorità e le esigenze dell'UE**, per raggiungere una capacità di reazione più flessibile, per sviluppare le capacità e competenze europee e rafforzare l'efficienza operativa e l'impatto globale dell'Agenzia. In questo modo l'ENISA potrebbe diventare una risorsa permanente per ciascuno Stato membro e l'Unione europea nel suo insieme*."

Il 18 dicembre 2009 il Consiglio ha adottato una risoluzione su un "*approccio europeo cooperativo in materia di sicurezza delle reti e dell'informazione*"[7], nella quale si sottolinea che "***l'ENISA, con un mandato riveduto, dovrebbe servire da centro di conoscenze dell'UE, per le tematiche connesse alla sicurezza delle reti e dell'informazione nell'ambito dell'UE***."

Una delle iniziative faro della strategia della Commissione "Europa 2020" per una crescita intelligente, sostenibile e inclusiva[8] è l'Agenda digitale europea, che riconosce un ruolo di primo piano alla sicurezza delle reti e dell'informazione. L'obiettivo dell'iniziativa strategica per accrescere la fiducia nell'Agenda digitale europea è consentire all'Unione europea, agli Stati membri e alle parti interessate di raggiungere un livello elevato di capacità e preparazione per prevenire, rilevare e reagire in modo più adeguato ai problemi legati alla sicurezza delle reti e dell'informazione. In tal modo si contribuirà ad aumentare la fiducia e la sicurezza nel mercato unico digitale europeo e la competitività delle aziende europee.

---

5 Dal 7 novembre 2008 al 9 gennaio 2009, relazione disponibile all'indirizzo: http://ec.europa.eu/information_society/policy/nis/nis_public_consultation/index_en.htm.

6 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Proteggere le infrastrutture critiche informatizzate" – COM (2009) 149 del 30.3.2009.

7 Risoluzione del Consiglio, del 18 dicembre 2009 , su un approccio europeo cooperativo in materia di sicurezza delle reti e dell'informazione (GU C 321 del 29.12.2009, pag. 1).

8 COM(2010) 2020.

2. DEFINIZIONE DEL PROBLEMA

2.1. Il problema

Sono stati individuati i seguenti problemi che rendono le parti interessate vulnerabili alle minacce e agli incidenti relativi alla sicurezza delle reti e dell'informazione. Tutti questi elementi dimostrano quanto sia necessaria una struttura affidabile, a livello di UE, per affrontare le difficoltà ed essere al passo con le tecnologie e le condizioni del mercato, in costante evoluzione in tutta Europa.

- **Differenze e frammentazione degli approcci nazionali.** I problemi legati alla sicurezza delle reti e dell'informazione superano i confini degli Stati e non possono essere affrontati in maniera efficace a livello esclusivamente nazionale. Allo stesso tempo, le autorità pubbliche dei vari Stati membri affrontano il problema in modi molto diversi. Per conformarsi alle molteplici prescrizioni in materia di sicurezza vigenti nei diversi Stati membri, le imprese che operano su tutto il territorio dell'UE devono sostenere dei costi che causano frammentazione e mancanza di competitività nel mercato interno europeo.

- **Limitata capacità europea di allarme rapido e di reazione.** I sistemi nazionali di allarme rapido e di reazione in caso di incidenti attualmente in uso variano enormemente da uno Stato membro all'altro e non esiste nessun sistema a livello di UE. Occorre quindi dotare l'Unione di strumenti strategici volti a individuare i rischi e le vulnerabilità in materia di sicurezza delle reti e dell'informazione, per istituire adeguati meccanismi di risposta e garantire che tali meccanismi siano conosciuti e utilizzati dalle parti interessate.

- **Carenza di dati affidabili e limitata conoscenza dei problemi in evoluzione.** Le informazioni quantitative affidabili sulle ripercussioni e persino sul verificarsi di incidenti legati alla sicurezza delle reti e dell'informazione sono molto scarse, per questo i responsabili delle politiche in materia hanno grosse difficoltà ad adottare misure adeguate e le imprese stentano a prendere decisioni in merito agli investimenti nella sicurezza.

- **Scarsa consapevolezza dei rischi e delle problematiche legate alla sicurezza delle reti e dell'informazione.** La responsabilità di garantire la sicurezza ricade sulle singole parti interessate, tuttavia tali responsabilità non sempre sono definite e comunicate in modo chiaro. Da un lato, i consumatori spesso sottovalutano i rischi e ignorano la propria responsabilità quando si tratta di rendere sicuri i loro sistemi informatici, dall'altro le imprese sovente considerano principalmente i costi legati alla sicurezza e non i risparmi potenziali che essa consente di ottenere.

- **Dimensione internazionale dei problemi legati alla sicurezza delle reti e dell'informazione.** Le minacce alla sicurezza e gli eventuali incidenti che ne conseguono hanno, per loro stessa natura, una portata internazionale. Le azioni dell'UE rischiano perciò di essere meno efficaci se i problemi non vengono affrontati su scala altrettanto ampia. Occorre mettere a punto una strategia e definire un punto di riferimento dell'UE in materia di sicurezza delle reti e dell'informazione per consolidare la posizione dell'Unione sulla scena internazionale.

- **Necessità di modelli di collaborazione per garantire un'adeguata attuazione della strategia.** A livello di UE sono necessari adeguati modelli di collaborazione per l'attuazione delle politiche in materia di sicurezza delle reti e dell'informazione. Le parti

interessate hanno bisogno di orientamenti per individuare le minacce e mettere a punto buone pratiche per l'attuazione delle politiche esistenti.

- **Necessità di azioni più efficaci contro la criminalità informatica.** Le azioni nel settore della sicurezza delle reti e dell'informazione sono state organizzate principalmente nell'ambito dell'ex "primo pilastro", ossia le questioni discusse tra le istituzioni. Con l'entrata in vigore del trattato di Lisbona, tuttavia, occorre tenere presente che un'agenzia che si occupi di sicurezza delle reti e dell'informazione deve avere un insieme di compiti più vasto che comprenda anche aree del secondo e terzo pilastro, ossia questioni sulle quali in precedenza decideva il Consiglio da solo.

2.2. Chi risente di più di questo problema?

Gli incidenti legati alla sicurezza delle reti e dell'informazione possono avere ripercussioni molto vaste su una serie di soggetti interessati, comprese piccole e grandi imprese, enti e amministrazioni pubbliche e singoli cittadini. In altre parole, la sicurezza delle reti e dell'informazione è un problema e una responsabilità di tutti.

Le informazioni quantitative oggettive disponibili in merito al numero esatto di incidenti e/o al loro impatto economico sono scarse o del tutto assenti. Secondo quando indicato nello studio di mercato IDC EMEA[9], negli ultimi 12 mesi il 28% delle famiglie nell'UE-27 ha avuto problemi di spam o virus informatici e in media circa il 7% degli utenti professionali (imprese) è incorso in un incidente legato alla sicurezza.

3. MOTIVI CHE GIUSTIFICANO UN'AZIONE A LIVELLO DI UE, VALORE AGGIUNTO E SUSSIDIARIETÀ

L'interdipendenza delle reti e dei sistemi di informazione rende molto difficile, se non impossibile, per le singole parti valutare appieno l'impatto sulla società e l'economia a livello mondiale delle misure adottate per prevenire gli incidenti legati alla sicurezza. La varietà di strategie e pratiche nazionali influisce sul mercato interno sia in negativo, in caso di incidenti (strategie inadeguate possono avere effetti sui mercati di altri Stati membri) sia in positivo, quando vengono attuate buone pratiche in materia di sicurezza (le buone pratiche applicate in uno Stato membro migliorano la sicurezza nel suo complesso, creando così un evidente vantaggio per la società). Un intervento strategico a livello di UE si giustifica quindi perché apporterebbe reale valore aggiunto al funzionamento del mercato interno, come riconosciuto dal regolamento (CE) n. 460/2004 che istituisce l'ENISA attribuendole competenze volte a contribuire al buon funzionamento del mercato interno.

L'intervento dell'UE in questo ambito è giustificato anche in base al *principio di sussidiarietà*. Come rilevato nella comunicazione CIIP, una strategia che preveda la totale assenza di intervento dell'UE nelle politiche nazionali in materia di sicurezza delle reti e dell'informazione equivarrebbe a chiedere a ciascuno Stato membro di vigilare esclusivamente sul proprio territorio, senza considerare l'interdipendenza dei sistemi informatici. Un'adeguata coordinazione tra gli Stati membri, volta a garantire che le implicazioni transfrontaliere dei rischi legati alla sicurezza possano essere affrontate in

[9] IDC EMEA, *The European Network and Information Security Market, Scenario, Trends and Challenges*, aprile 2009, con riferimenti allo studio Eurobarometro sulle comunicazioni elettroniche, aprile 2007.

maniera adeguata, è perciò conforme al principio di sussidiarietà. Inoltre, l'azione dell'UE rafforzerebbe l'efficacia delle politiche nazionali esistenti.

I cittadini dell'Unione affidano sempre di più i propri dati a sistemi informatici complessi (ad es. il *cloud computing*). Per questo un'azione strategica coordinata e collaborativa nell'ambito della sicurezza delle reti e dell'informazione può avere ripercussioni estremamente positive ai fini di un'effettiva *tutela dei diritti fondamentali*, in particolare il diritto alla *protezione dei dati personali e della riservatezza*. Anche per questa ragione un'ulteriore azione dell'UE sembra ampiamente giustificata.

4. OBIETTIVI STRATEGICI

La presente valutazione dell'impatto intende determinare in che modo debba essere strutturata un'agenzia modernizzata responsabile della sicurezza delle reti e dell'informazione (ampiamente riconosciuta come struttura organizzativa più adeguata) per contribuire, insieme ad altri strumenti dell'Unione, a raggiungere gli obiettivi della politica in materia di sicurezza delle reti e dell'informazione.

L'obiettivo generale è consentire all'Unione europea, agli Stati membri e alle parti interessate di raggiungere un livello elevato di capacità e preparazione per prevenire, rilevare e reagire in modo più adeguato ai problemi legati alla sicurezza delle reti e dell'informazione. In tal modo si contribuirà ad aumentare la fiducia nel mercato unico digitale europeo e la competitività delle aziende europee.

Questo obiettivo generale si suddivide in sette **obiettivi specifici**:

(1) **Coerenza degli approcci normativi** – fornire orientamenti e consulenza alla Commissione e agli Stati membri per l'aggiornamento e la definizione di un quadro normativo globale nel campo della sicurezza delle reti e dell'informazione.

(2) **Prevenzione, rilevamento e reazione** – migliorare la preparazione contribuendo alla capacità europea di allarme rapido e di reazione in caso di incidenti e alla messa a punto di piani ed esercizi di emergenza paneuropei.

(3) **Sostegno all'elaborazione di politiche** – fornire assistenza e consulenza alla Commissione e agli Stati membri.

(4) **Responsabilizzazione delle parti interessate** – sviluppare una cultura della sicurezza e della gestione dei rischi favorendo la condivisione di informazioni e la cooperazione tra le parti sia del settore pubblico che di quello privato, anche a diretto vantaggio dei cittadini e delle PMI, e favorire il diffondersi di una cultura in materia di sicurezza delle reti e dell'informazione.

(5) **Partecipazione attiva dell'Europa sulla scena internazionale** – raggiungere un alto livello di cooperazione con i paesi terzi e le organizzazioni internazionali per promuovere un approccio comune alla sicurezza su scala mondiale e incoraggiare iniziative internazionali di alto livello in Europa.

(6) **Collaborazione ai fini dell'attuazione** – facilitare la collaborazione nell'attuazione delle politiche in materia di sicurezza delle reti e dell'informazione.

(7) **Lotta contro la criminalità informatica** – mettere a punto meccanismi di reazione efficaci ai crimini informatici legati alla sicurezza delle reti e dell'informazione, in

collaborazione con le autorità che attengono agli ex-pilastri secondo e terzo (ad es. Europol).

5. POSSIBILI FORME ORGANIZZATIVE E OPZIONI STRATEGICHE

Nella valutazione d'impatto (capo 4 e allegato 4) sono esaminate diverse possibili forme organizzative per attuare le opzioni strategiche elencate sopra, tra le quali: i) un'agenzia, ii) un partenariato pubblico-privato (PPP) più o meno formalizzato, iii) una rete di contatto informale, iv) una rete permanente di enti competenti e v) l'integrazione completa in un servizio della Commissione.

Dal confronto tra queste diverse forme organizzative, l'Agenzia sembra emergere come strumento più adeguato per i vantaggi che offre in relazione ai seguenti aspetti: 1) sicurezza giuridica della struttura organizzativa e del suo contenuto, 2) adeguatezza alle problematiche specifiche di un settore delicato come quello della sicurezza delle reti e dell'informazione (organo che raggruppa esperti esterni, coordinamento delle relazioni con le parti interessate, coinvolgimento/impegno degli Stati membri) e 3) accettazione e reputazione dell'ENISA nel settore.

Per questo motivo, sono state sviluppate e attentamente valutate le seguenti opzioni relative alla forma organizzativa di un'agenzia.

Opzione strategica 1: Nessuna politica

Questa opzione presuppone che l'ENISA cessi di esistere dopo marzo 2012 e che nessun'altra istituzione europea si faccia carico, interamente o in parte, delle attività attualmente svolte dall'Agenzia.

Chiudere l'ENISA significherebbe che tutte le risorse investite finora per creare un organismo in grado di attirare collaboratori altamente specializzati, acquisire esperienza e creare reti con e tra le parti interessate e le istituzioni internazionali, verrebbero meno proprio nel momento in cui l'attuale Agenzia ha raggiunto la sua piena capacità operativa.

La natura complessa delle problematiche legate alla sicurezza delle reti in tutta Europa richiede un'Agenzia modernizzata e rafforzata e non giustifica la chiusura di quella esistente. Ciò è confermato anche dal ruolo espressamente affidato all'ENISA, ad esempio nel quadro normativo rivisto per le comunicazioni elettroniche[10] e dal sostegno generalmente espresso dalle parti interessate, in favore di un ruolo più importante per un'agenzia europea per la sicurezza delle reti e dell'informazione.

Opzione strategica 2: Status quo

L'opzione 2 corrisponde a uno scenario immutato, nel quale lo strumento esistente viene mantenuto in forma identica e con le medesime risorse. Le parti interessate sono concordi nel ritenere che l'ENISA è diventata un punto di riferimento autorevole per le questioni inerenti la sicurezza delle reti e dell'informazione e che si è imposta come centro di eccellenza in questo ambito.

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

Con le restrizioni attuali in materia di personale e di bilancio, l'impatto dell'Agenzia sarebbe limitato ad un numero molto contenuto di aspetti legati alla sicurezza. Questo, però, è in contrasto con le aspettative generali delle parti interessate. Se non si consente all'Agenzia di evolvere ed essere all'altezza delle crescenti aspettative, potrebbe a un certo punto venire meno la sua credibilità.

Opzione strategica 3: Ampliare le funzioni attuali dell'ENISA e includere le agenzie incaricate del rispetto delle norme e della tutela della riservatezza come parti interessate a pieno titolo

Questa opzione prevede un ampliamento del ruolo dell'Agenzia, in particolare per quanto riguarda:

- creare e mantenere una rete di contatti tra le parti interessate e una rete di conoscenze;
- servire da centro di supporto per lo sviluppo e l'attuazione delle strategie in materia di sicurezza delle reti e dell'informazione (in particolare per quanto riguarda la riservatezza online, la firma elettronica, l'identificazione elettronica e le norme sugli appalti pubblici relative alla sicurezza);
- sostenere la politica dell'UE in materia di infrastrutture critiche informatizzate e resilienza (ad es. esercizi, EP3R[11], il sistema europeo di condivisione delle informazioni e di allarme, ecc.)
- creare un quadro a livello di UE per la raccolta di dati relativi alla sicurezza delle reti e dell'informazione, anche mettendo a punto metodi e pratiche per la notifica legale e la condivisione di tali dati;
- studiare l'economia della sicurezza delle reti e dell'informazione e renderne conto;
- favorire la cooperazione con i paesi terzi e le organizzazioni internazionali per promuovere un approccio comune globale alla sicurezza delle reti e dell'informazione e avere un impatto sulle iniziative internazionali di alto livello in Europa;
- svolgere compiti non operativi legati agli aspetti dell'applicazione delle norme e della cooperazione giudiziaria.

L'Agenzia disporrebbe di tutte le risorse necessarie per adempiere a questi compiti in modo soddisfacente e approfondito, avendo così un impatto reale. Disponendo di maggiori risorse, l'ENISA potrebbe avere un ruolo più attivo e prendere iniziative per favorire la partecipazione delle parti interessate. Inoltre, la nuova situazione consentirebbe una maggiore flessibilità per reagire rapidamente ai costanti cambiamenti nel campo della sicurezza delle reti.

Opzione strategica 4: Attribuire ulteriori funzioni operative per la lotta contro gli attacchi informatici e la reazione agli incidenti informatici

Oltre alle attività previste dall'opzione 3 l'Agenzia avrebbe funzioni operative, quali un ruolo più attivo nelle infrastrutture critiche informatizzate dell'UE, ad esempio per quanto riguarda la prevenzione e la reazione agli incidenti, agendo in qualità di squadra di pronto intervento informatico (CERT) per quanto riguarda la sicurezza delle reti e dell'informazione, svolgendo anche attività di gestione corrente e servizi di reazione alle emergenze.

Questa opzione richiederebbe un aumento sostanziale del bilancio e delle risorse umane a

[11] Partenariati pubblico-privati europei per la resilienza, COM (2009)149.

disposizione dell'Agenzia. Questo pone problemi in termini di capacità di assorbimento e uso efficace del bilancio in rapporto ai benefici ottenuti.

Opzione strategica 5: Aggiungere funzioni operative che consistono nel prestare assistenza alle autorità giudiziarie e di polizia nella lotta contro la criminalità informatica

Oltre alle attività previste dall'opzione 4, questo scenario comprende funzioni relative a:

- fornire sostegno in materia di diritto procedurale (cfr. convenzione sulla criminalità informatica): ad es. raccolta di dati sul traffico, intercettazione di dati sui contenuti, monitoraggio dei flussi in caso di attacchi di *denial-of-service*;
- servire da centro di competenze per le indagini giudiziarie che presentano aspetti legati alla sicurezza delle reti e dell'informazione.

Come nello scenario precedente, questa opzione presuppone un aumento sostanziale delle risorse dell'Agenzia e solleva preoccupazioni simili riguardo alla capacità di assorbimento e all'uso efficace del bilancio.

6. CONFRONTO DELLE OPZIONI E VALUTAZIONE DEGLI IMPATTI

L'analisi dei possibili impatti economici, sociali e ambientali mostra che l'**opzione 1** avrebbe effetti negativi sotto ogni aspetto e causerebbe un peggioramento della situazione.

L'**opzione 2** non appare ottimale perché l'Agenzia non disporrebbe delle risorse necessarie per affrontare adeguatamente le difficoltà poste da uno scenario in costante cambiamento; potrebbero quindi derivarne danni alla reputazione e, a lungo termine, un crollo della credibilità dell'Agenzia.

Applicando l'**opzione 3**, un'Agenzia modernizzata contribuirebbe a:

Ridurre la frammentazione degli approcci nazionali (problema 1), agevolare l'elaborazione di strategie e il processo decisionale sulla base di dati, conoscenze e informazioni (problema 3), aumentare la consapevolezza dei rischi e dei problemi inerenti la sicurezza delle reti e dell'informazione (problema 4) e affrontarli, contribuendo a:

- raccogliere in maniera più efficace le informazioni rilevanti relative ai rischi, alle minacce e alle vulnerabilità in ciascuno Stato membro;
- rendere disponibili maggiori informazioni sui rischi e le sfide attuali e future in questo settore;
- permettere agli Stati membri di elaborare strategie più raffinate in materia di sicurezza delle reti e dell'informazione.

Migliorare i sistemi di allarme rapido e la capacità di reazione dell'Europa (problema 2):

- aiutando la Commissione e gli Stati membri ad organizzare esercizi paneuropei e realizzando in tal modo economie di scala per quanto riguarda la reazione agli incidenti che interessano tutta l'UE;
- facilitando il funzionamento dei partenariati pubblico-privato (EP3R) che potrebbero attirare investimenti favoriti dall'esistenza di obiettivi strategici

comuni e di norme valide in tutta l'UE nel settore della sicurezza e della resilienza.

Promuovere un approccio comune globale alla sicurezza delle reti e dell'informazione (problema 5):

- aumentando lo scambio di informazioni e conoscenze con i paesi terzi.

Contrastare la criminalità informatica in maniera più efficace (problema 7):

- con il coinvolgimento in compiti non operativi legati alla sicurezza delle reti nell'ambito dell'applicazione delle norme e della cooperazione giudiziaria, come lo scambio reciproco di informazioni e formazione (ad es. in collaborazione con l'Accademia europea di polizia - AEP).

L'***opzione 4*** avrebbe un impatto maggiore a livello operativo, in aggiunta agli effetti previsti per l'opzione 3. Agendo come CERT dell'UE in materia di sicurezza delle reti e dell'informazione e coordinando le CERT nazionali, l'Agenzia contribuirebbe a conseguire maggiori economie di scala nella reazione agli incidenti che interessano tutta l'UE e a ridurre i rischi operativi per le imprese, ad esempio aumentando il livello della sicurezza e della resilienza.

L'***opzione 5*** permetterebbe di contrastare più efficacemente la criminalità informatica rispetto alle opzioni 3 e 4, con l'aggiunta di funzioni operative a sostegno delle autorità giudiziarie e di polizia.

Tuttavia, nonostante il più ampio impatto positivo rispetto all'opzione 3, le opzioni 4 e 5 sarebbero delicate dal punto di vista politico per gli Stati membri per via delle responsabilità che comportano in relazione alle infrastrutture critiche informatizzate (diversi Stati membri non sarebbero favorevoli ad un accentramento delle funzioni operative). Inoltre, il mandato più ampio previsto dalle opzioni 4 e 5 potrebbe rendere meno chiara la posizione dell'Agenzia. L'aggiunta di questi ed altri compiti operativi completamente diversi potrebbe causare molte difficoltà nel breve periodo, con il rischio concreto che l'Agenzia non sia in grado di svolgere adeguatamente questo genere di compiti entro un arco di tempo ragionevole. Infine, l'attuazione delle opzioni 4 e 5 avrebbe costi estremamente elevati - sarebbe infatti necessario assegnare all'ENISA un bilancio di quattro o cinque volte superiore rispetto a quello attuale.

Mettendo a confronto gli impatti delle cinque opzioni relative alla forma organizzativa di un'agenzia modernizzata per la sicurezza delle reti e dell'informazione, le opzioni 1 e 2 devono essere scartate perché non consentirebbero di affrontare adeguatamente le problematiche in oggetto a livello europeo. Gli scenari 3, 4 e 5, invece, consentirebbero all'UE di affrontare in maniera adeguata le future opzioni strategiche in materia. Al momento attuale le opzioni 4 e 5 appaiono troppo ambiziose, sia per quanto riguarda le implicazioni politiche nella maggior parte degli Stati membri, sia per quanto riguarda l'aspetto del bilancio. Pertanto, ***l'opzione 3 risulta la più adatta per affrontare nel modo più efficace i sette problemi individuati in relazione alla sicurezza delle reti e dell'informazione***.

7. CONTROLLO E VALUTAZIONE: COME MISURARE I COSTI E I BENEFICI EFFETTIVI E IL CONSEGUIMENTO DEGLI EFFETTI DESIDERATI?

Questa iniziativa strategica prevede valutazioni periodiche che sarebbero trasmesse dalla Commissione al Parlamento europeo e al Consiglio e rese pubbliche. Le valutazioni terrebbero conto delle opinioni delle parti interessate pertinenti, sulla base del mandato concordato con il consiglio di amministrazione dell'Agenzia, valuterebbero l'efficacia dell'Agenzia nel raggiungere gli obiettivi fissati e servirebbero a determinare se l'Agenzia continua ad essere uno strumento efficace e se siano necessarie modifiche al suo mandato e/o ad altri elementi del regolamento che la istituisce. In seguito alla valutazione il consiglio di amministrazione dell'Agenzia elaborerebbe delle raccomandazioni destinate alla Commissione in relazione alle eventuali modifiche da apportare al regolamento. Il consiglio di amministrazione e il direttore esecutivo dell'Agenzia dovrebbero tenere conto dei risultati delle valutazioni in sede di pianificazione pluriennale delle attività dell'Agenzia.

L'operato dell'Agenzia è sottoposto al controllo del mediatore, a norma delle disposizioni dell'articolo 228 del trattato.