STRATEGIA DELL'UE PER LA CYBERSECURITY PER IL DECENNIO DIGITALE

VITTORIO CALAPRICE – RAPPRESENTANZA IN ITALIA DELLA COMMISSIONE EUROPEA

DI COSA PARLEREMO

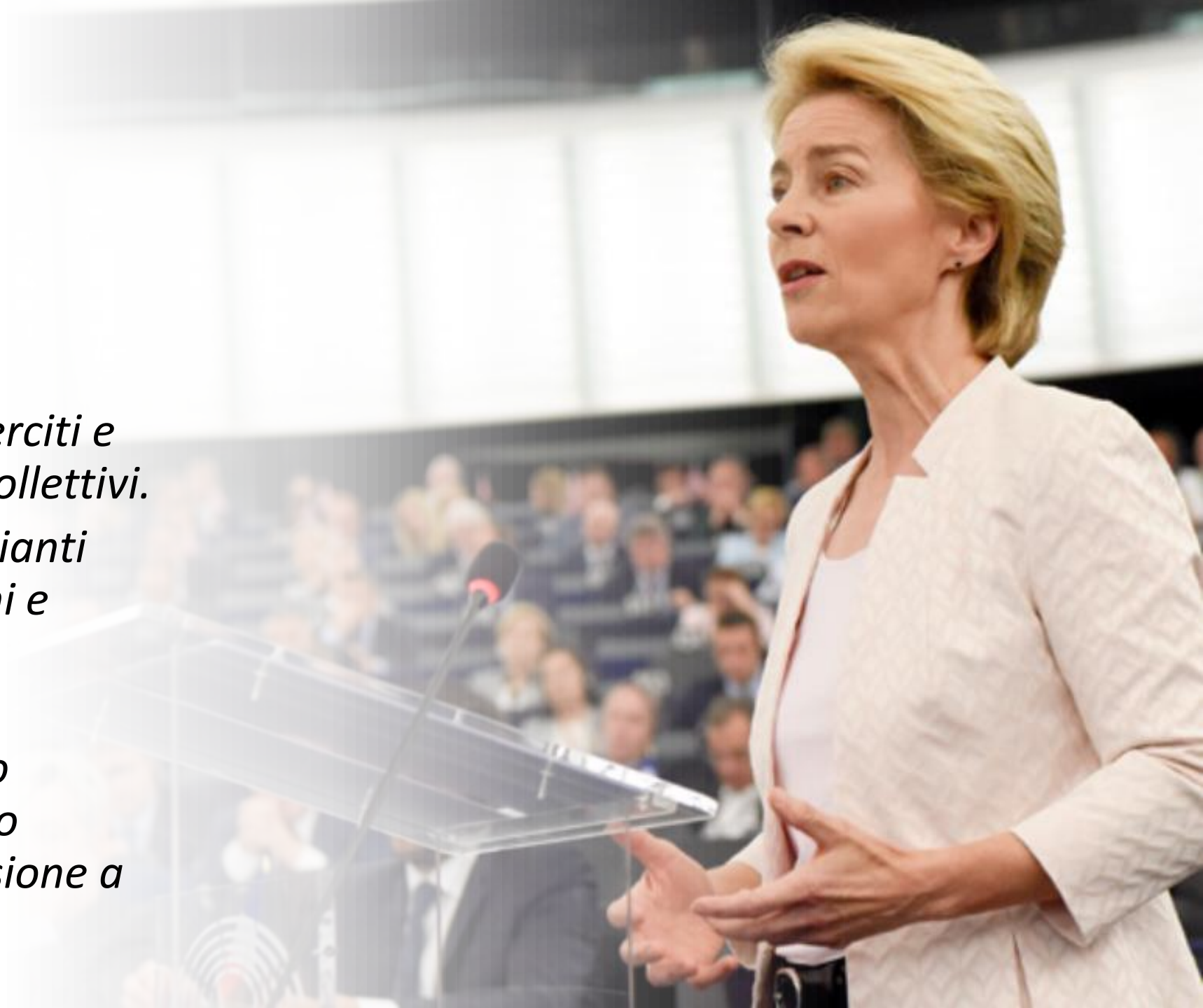
- I 3 assi della strategia europea per la cybersecurity
- information sharing, PPP, Cybersecurity ACT, Digital Europe
- Joint Cyber Unit, Cybershield, European Cybersecurity Competence Center

Dal Discorso sullo Stato dell'Unione al Parlamento europeo, 15 settembre 2021

Non sono più necessari eserciti e missili per causare danni collettivi.

Si possono paralizzare impianti industriali, amministrazioni e ospedali con un semplice computer portatile.

Si può perturbare un intero processo elettorale con uno smartphone e una connessione a Internet.



Dal Discorso sullo Stato dell'Unione al Parlamento europeo, 15 settembre 2021

Se tutto è collegato, tutto può essere piratato. Dato che le risorse sono scarse, dobbiamo unire le nostre forze.

E non dovremmo limitarci ad affrontare le minacce informatiche, ma dovremmo cercare anche di conquistare un posto di primo piano nella ***cibersicurezza […]***

Perciò abbiamo bisogno di una politica europea della ciberdifesa, compresa una legislazione su norme comuni nel quadro di una nuova ***legge europea sulla ciberresilienza***

European Commission

Nel dicembre del 2020 la Commissione e l'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato **una nuova strategia dell'UE per la cibersicurezza**

LA STRATEGIA EUROPEA PER LA CYBERSECURITY

LA CYBERSECURITY AL CENTRO DELLO SPAZIO DIGITALE UE

Essa contiene proposte e iniziative politiche, di regolamentazione e di investimento in **3 aree d'azione dell'UE:**

1.resilienza, sovranità tecnologica e leadership;

2.Sviluppo della capacità operativa di prevenzione, deterrenza e risposta;

3.Promozione di un ciberspazio globale e aperto grazie a una maggiore cooperazione

Infrastrutture critiche europee e cyberisk

Le strutture ospedaliere, reti energetiche, ferrovie, ma anche centri dati, amministrazioni pubbliche, laboratori di ricerca e produzione di dispositivi medici e medicinali, nonché altre infrastrutture e servizi essenziali devono rimanere **impermeabili in un contesto di minacce sempre più repentine e complesse.**

IoT ed Infrastrutture critiche

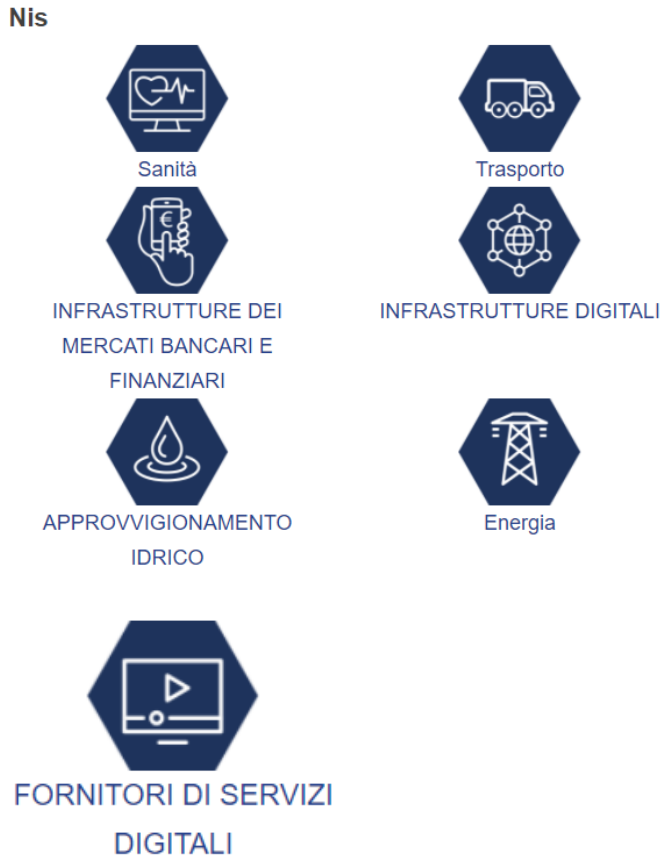
DALLA NIS ALLA NIS2

In questa linea d'azione la Commissione ha proposto di **riformare le norme sulla sicurezza delle reti e dei sistemi informatici** per un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista o "NIS 2") al fine di aumentare il livello di ciberresilienza dei settori pubblici e privati essenziali.

LE NUOVE NORME DELLA NIS 2:

1. **rafforzeranno** gli obblighi di sicurezza per le imprese
2. si occuperanno della sicurezza delle **catene di approvvigionamento**
3. introdurranno **misure di vigilanza** più rigorose per le autorità nazionali
4. accresceranno ulteriormente la **condivisione delle informazioni** e la cooperazione

ATTUALI SETTORI CONTEMPLATI DALLA DIRETTIVA NIS



FUTURI SETTORI CONTEMPLATI DALLA DIRETTIVA NIS 2

PRODUZIONE DI ALCUNI PRODOTTI CRITICI (COME PRODOTTI FARMACEUTICI, DISPOSITIVI MEDICI, PRODOTTI CHIMICI)

SERVIZI POSTALI E DI CORRIERE

Cibo

PUBBLICA AMMINISTRAZIONE

FORNITORI DI RETI O SERVIZI PUBBLICI DI COMUNICAZIONE ELETTRONICA

SERVIZI DIGITALI COME PIATTAFORME DI SERVIZI DI SOCIAL NETWORKING E SERVIZI DI DATA CENTER

GESTIONE DELLE ACQUE REFLUE E DEI RIFIUTI

Spazio

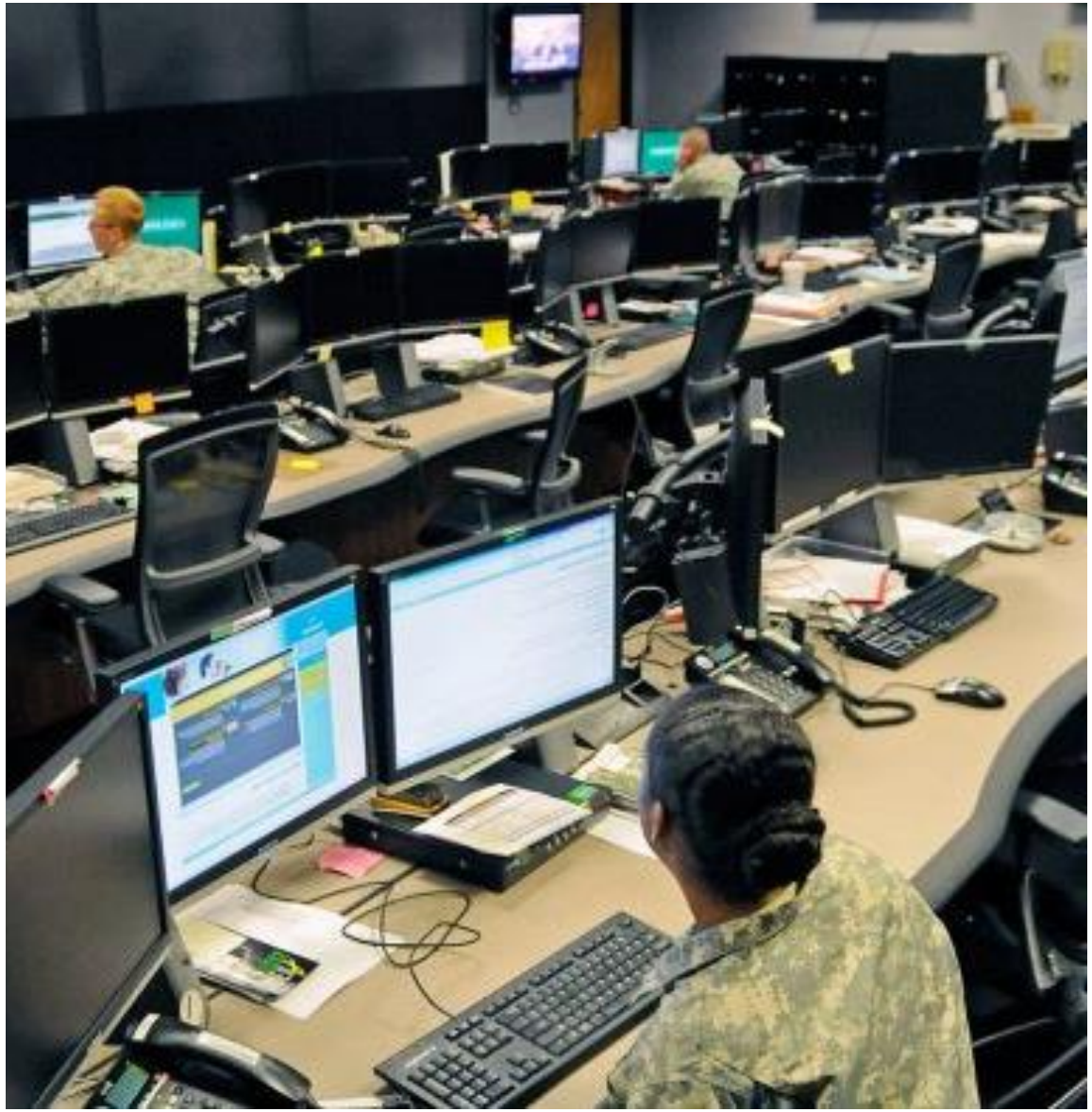
1. CREAZIONE DELLA RESILIENZA, SOVRANITÀ TECNOLOGICA E LEADERSHIP

costituzione di un centro **europeo di competenza industriale, tecnologica e di ricerca sulla cybersicurezza** insieme ad una rete di centri nazionali di coordinamento;

contributo del settore industriale e del mondo accademico **per sviluppare la sovranità tecnologica dell'UE** in materia di sicurezza informatica, **garantire la sicurezza di infrastrutture** e **sostenere la ricerca e l'innovazione** per ridurre la dipendenza esterna per le tecnologie

2. COSTRUZIONE DI UNA CAPACITA OPERATIVA DI PREVENZIONE, DISSUASIONE E RISPOSTA

Nell'ambito del secondo indirizzo è stata prevista la creazione di una **Unità Cibernetica Congiunta (Joint Cyber Unit)**, nella forma di una **piattaforma fisica e virtuale** per la cooperazione tra le varie autorità di cybersecurity all'interno dell'UE, per dare una risposta coordinata ed efficace agli attacchi anche attraverso la **creazione di partenariati strutturati pubblico/privati**



3. PROMOZIONE DI UNO SPAZIO CIBERNETICO GLOBALE E APERTO ATTRAVERSO UNA MAGGIORE COOPERAZIONE

La Commissione e l'Alto Rappresentante rafforzeranno la comunicazione con i portatori di interessi, compreso il settore privato, il mondo accademico e la società civile: **l'interdipendenza dello spazio cibernetico coinvolge tutti e nessuno è esente dalla responsabilità di renderlo uno spazio globale, aperto e sicuro rafforzando la resilienza collettiva dell'Europa contro le minacce informatiche.**

IN CHE MODO L'UE REALIZZERÀ UN CIBERSPAZIO GLOBALE, APERTO, STABILE E SICURO?

L’UE sta intensificando i lavori per rafforzare l'ordine mondiale basato su regole, promuovere la sicurezza e la stabilità internazionali nel ciberspazio e proteggere i diritti umani e le libertà fondamentali online.

Promuoverà norme e standard internazionali che riflettano tali valori fondamentali dell'UE collaborando con i suoi partner internazionali nelle Nazioni Unite e in altre sedi pertinenti.

un **pacchetto di strumenti** dell'UE per la diplomazia informatica rafforzato al fine di prevenire e scoraggiare gli attacchi informatici e rispondervi;

una **cooperazione rafforzata nell'ambito della cyberdifesa**, in particolare attraverso la revisione del quadro strategico in materia di ciberdifesa;

STRUMENTI PER L'AZIONE ESTERNA DELLA STRATEGIA EU PER LA CYBERSECURITY

- Information sharing & Partenariato Pubblico Privato
- Cybersecurity ACT e Certificazione europea
- Programma Digital Europe

LA CONDIVISIONE DELLE INFORMAZIONI NELLA SICUREZZA INFORMATICA

- Per combattere in modo efficiente le minacce informatiche in evoluzione, la condivisione delle informazioni è senza dubbio una risorsa preziosa.

- Con il progresso tecnologico, vengono registrati livelli crescenti di incidenti di sicurezza informatica. La gravità e l'entità di questi attacchi possono avere un **impatto sostanziale sulla sicurezza nazionale di un paese**.

- Uno degli obiettivi principali dei Governi è proteggere la sicurezza nazionale promuovendo la **condivisione delle informazioni tra il settore privato e quello pubblico.**

IL VANTAGGIO DELLA CONDIVISIONE DELLE INFORMAZIONI

Ai fini della prevenzione delle intrusioni, è necessario disporre di dati in tempo reale su un attacco informatico. Ciò consente ai difensori di anticipare l'approccio degli aggressori e adottare misure strategiche in tempo.

Ciò migliora le pratiche di **Cybersecurity Incidence Response** e scoraggia gli aggressori. I professionisti della sicurezza informatica in tutto il mondo supportano la condivisione delle informazioni come migliore intelligence per gestire gli attacchi informatici.

- i centri di condivisione e di analisi delle informazioni (ISAC) aiutano le parti interessate dell'industria e le autorità pubbliche a scambiarsi informazioni sulle minacce

- necessario monitorare costantemente le reti e i sistemi informatici per rilevare le intrusioni e le anomalie in tempo reale

L'UE HA BISOGNO DI INDIVIDUARE E RESPINGERE GLI ATTACCHI INFORMATICI

Il Partenariato Pubblico-Privato: nozione

Il PPP uno strumento di collaborazione e/o cooperazione a lungo termine fra il settore privato e quello pubblico, il quale può essere impiegato in diverse aree.

In particolare, questa tipologia di rapporto è stata largamente utilizzata nei settori delle opere pubbliche, come quello del trasporto e delle infrastrutture

IL PPP NELLA CYBERSECURITY

A livello europeo è relativamente recente l'accostamento dei PPP al mondo della cyber security.

La strategia per il Mercato Unico digitale in Europa ha evidenziato la necessità di creare un **partenariato pubblico privato sulla cibersicurezza** nel settore delle tecnologie e soluzioni per le sicurezza di rete.

Nel 2016 istituzione dell'**Organizzazione Europea per la Cyber Security (ECSO)** Informatica (ECSO).

PPP : QUANTO SI PREVEDE DI INVESTIRE NELLA CIBERSICUREZZA?

Nell'ambito del quadro finanziario pluriennale 2021-2027 sono previsti finanziamenti dell'UE nella cibersicurezza dal programma **Europa Digitale** e nella ricerca sulla cibersicurezza dal programma **Orizzonte Europa,** con particolare attenzione al sostegno alle piccole e medie imprese (PMI), per un totale che potrebbe ammontare a **20 miliardi di euro** a cui si aggiungeranno gli investimenti degli **Stati membri e dell'industria.**

IL CYBERSECURITY ACT

Il Cybersecurity Act è un Regolamento del 2019 voluto dalla Commissione europea per rafforzare la sicurezza informatica dei prodotti ICT e dei servizi digitali in Europa.

IL CYBERSECURITY ACT TRATTA PRINCIPALMENTE DUE ARGOMENTI:

1. Il rafforzamento del mandato dell'**ENISA,** Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione. L'Agenzia assume un ruolo diretto nella prevenzione dei cyber-attacchi, rafforzando la propria posizione.

2. La definizione del **quadro europeo delle certificazioni in ambito sicurezza informatica.** In altre parole vengono tracciati standard – validi in tutto il territorio UE – con cui valutare se prodotti e servizi IT siano effettivamente sicuri e certificabili.

Cybersecurity Act: definizione del quadro europeo di certificazione della cybersecurity

a) Il secondo punto chiave del Cybersecurity Act riguarda l'istituzione di un **quadro europeo di certificazione della cyber-sicurezza** di prodotti e servizi digitali.
b) Questo provvedimento ha il fine di facilitare lo scambio e il commercio di tutti prodotti ICT all'interno dell'UE **definendo degli standard universali, validi per tutti gli Stati membri.**
c) Grazie all'istituzione di queste certificazioni, sarà possibile creare un **mercato interno all'UE di prodotti e servizi informatici sicuri e certificati.**

Certificazione negli Stati membri

- Esistono già, infatti, degli standard di certificazione di sicurezza informatica validi per ciascuno Stato, ma non esiste un quadro universale di giudizio all'interno di tutto il territorio UE.

- Le imprese che desiderano creare un giro d'affari transnazionale sono spesso costrette a certificare i propri prodotti/servizi più volte. Per esempio, le certificazioni informatiche valide per la Germania non risultano valide per la Francia. Di conseguenza, un'azienda presente in entrambi gli Stati dovrà certificare i propri prodotti due volte, incrementando notevolmente i costi (una certificazione può arrivare a costare anche 1 milione di Euro).

Il programma Europa Digitale per il periodo 2021 – 2027

Il programma Europa digitale finanzia progetti in cinque settori cruciali:

- supercalcolo
- intelligenza artificiale
- cibersicurezza
- competenze digitali avanzate
- garantire un uso diffuso delle tecnologie digitali nell'economia e nella società.

6 June 2018

INVESTING IN THE FUTURE
DIGITAL TRANSFORMATION 2021-2027

WHY IS THIS A PRIORITY?

Digital transformation holds the key to unlocking future growth in Europe. Through new funding projects, the next long-term EU budget – the European Multiannual Financial Framework - will help to bridge the EU's digital investment gap for the 2021-2027 period.

I finanziamenti per cybersecurity provenienti da DIGITAL EUROPE

- Il programma mira a colmare il divario tra la **ricerca** sulle tecnologie digitali e la **diffusione** sul mercato a beneficio dei cittadini e delle imprese europee, in particolare le PMI.

- Gli investimenti nell'ambito del programma Europa digitale sosterranno il **duplice obiettivo** dell'Unione europea della **transizione verde** e della **trasformazione digitale** nonché rafforzare la **resilienza e la sovranità digitale** dell'Unione.

The Commission has created a **new Digital Europe programme** with an overall budget of **€9.2 billion** to shape and support the digital transformation of Europe's societies and economies. The programme will boost frontline investments in supercomputing, artificial intelligence, cybersecurity and advanced digital skills.

FIVE FOCUS AREAS UNDER DIGITAL EUROPE PROGRAMME:

pdated 05 June 2018

Cybershield

Joint Cyber Unit

Cyber Competence Center

CYBER-SHIELD

La Commissione ha proposto di istituire una **rete di centri operativi di sicurezza** dell'UE e di sostenere il miglioramento dei **centri esistenti e la creazione di nuovi,** nonché la formazione e lo sviluppo delle competenze del personale che li gestisce.

INTELLIGENZA ARTIFICIALE AL SERVIZIO DELLA CYBERSECURITY

Il Cyber-scudo a livello dell'UE sarà composto da centri operativi di sicurezza che utilizzano l'Intelligenza Artificiale e l'apprendimento automatico per **rilevare precocemente segnali** di attacchi informatici imminenti e consentire di intervenire **prima che si verifichino danni**

Sviluppo di uno scudo informatico europeo attraverso una rete di centri operativi di sicurezza abilitati all'intelligenza artificiale in grado di rilevare segni di attacco informatico e consentire azioni preventive prima che si verifichino danni

IL CYBER COMPETENCE CENTER EUROPEO 1/2

Il regolamento che istituisce un nuovo Centro di competenza per la cibersicurezza e una rete di centri nazionali di coordinamento è entrato in vigore nel giugno del 2021.

IL CYBERSECURITY COMPETENCE CENTER 2/2

Il Centro di competenza per la cibersicurezza avrà sede a **Bucarest,** contribuirà a rafforzare le capacità europee di cibersicurezza e a promuovere l'eccellenza della ricerca e la competitività dell'industria dell'Unione nel settore della cibersicurezza.

PER RICAPITOLARE

i settori della strategia UE per la cybersecurity:

- **Resilienza**
- **Attività di contrasto e applicazione della legge**
- **Diplomazia**
- **Difesa.**

RESILIENZA (1 / 2): PRINCIPALI PROTAGONISTI

- **Agenzia dell'Unione europea per la cibersicurezza (ENISA)**

Un centro di competenza in materia di cibersicurezza nell'UE: contribuisce, tra l'altro, alla cooperazione operativa nell'Unione, allo sviluppo delle capacità, alla sensibilizzazione e all'istruzione.

- **Squadra di risposta alle emergenze informatiche per le istituzioni, gli organi e le agenzie dell'UE (CERT-EU)**

Composto da esperti di sicurezza informatica delle principali istituzioni dell'UE.

- **National Computer Security Incident Response Teams (CSIRTs)**

Composto da esperti tecnici di cibersicurezza nominati dai CSIRT degli Stati membri dell'UE e dal CERT-EU: promuove una cooperazione rapida ed efficace.

RESILIENZA (2 / 2): PRINCIPALI PROTAGONISTI

- **Rete dell'UE per il collegamento in materia di crisi cibernetica (CyCLONe)**

Composto da esperti operativi di gestione delle crisi degli Stati membri: garantisce che le informazioni fluiscano efficacemente dal livello tecnico ai responsabili politici.

- **Gruppo di cooperazione per la sicurezza delle reti e dei sistemi d'informazione**

Composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA: facilita la cooperazione strategica sulle politiche in materia di cibersicurezza nell'UE.

- **Centri operativi di sicurezza (SOC)**

Un team di sicurezza delle informazioni che monitora, analizza e affronta gli incidenti di sicurezza informatica e i rischi di un'organizzazione, sia pubblici che privati. Combina risorse e procedure umane e tecnologiche. I SOC spesso collaborano strettamente con i team di risposta alle emergenze informatiche per garantire che gli incidenti di sicurezza informatica siano affrontati in modo efficace.

Istituita nell'ambito di Europol, comprende la task force congiunta sulla criminalità informatica (J-CAT) e funge da punto focale nella lotta contro la criminalità informatica nell'Unione.

APPLICAZIONE DELLA LEGGE : IL CENTRO EUROPEO PER LA CRIMINALITÀ INFORMATICA (EC3)

Cyber - Diplomazia

- **Servizio europeo per l'azione esterna (SEAE)**

Contribuisce alla promozione e alla protezione di un ciberspazio globale, aperto, stabile e sicuro. Attraverso la "**Cyber Diplomacy Toolbox**" fornisce supporto nell'utilizzo dell'intera gamma di misure diplomatiche, in particolare per quanto riguarda la comunicazione pubblica, sostenendo la consapevolezza condivisa e l'impegno con i paesi terzi in caso di crisi.

- **Gruppo di lavoro orizzontale sulle questioni informatiche**

Un forum che discute, tra gli altri argomenti, l'utilizzo di misure nell'ambito della Cyber Diplomacy Toolbox: un quadro per una risposta diplomatica congiunta dell'UE alle attività informatiche dannose.

CYBER -DIFESA

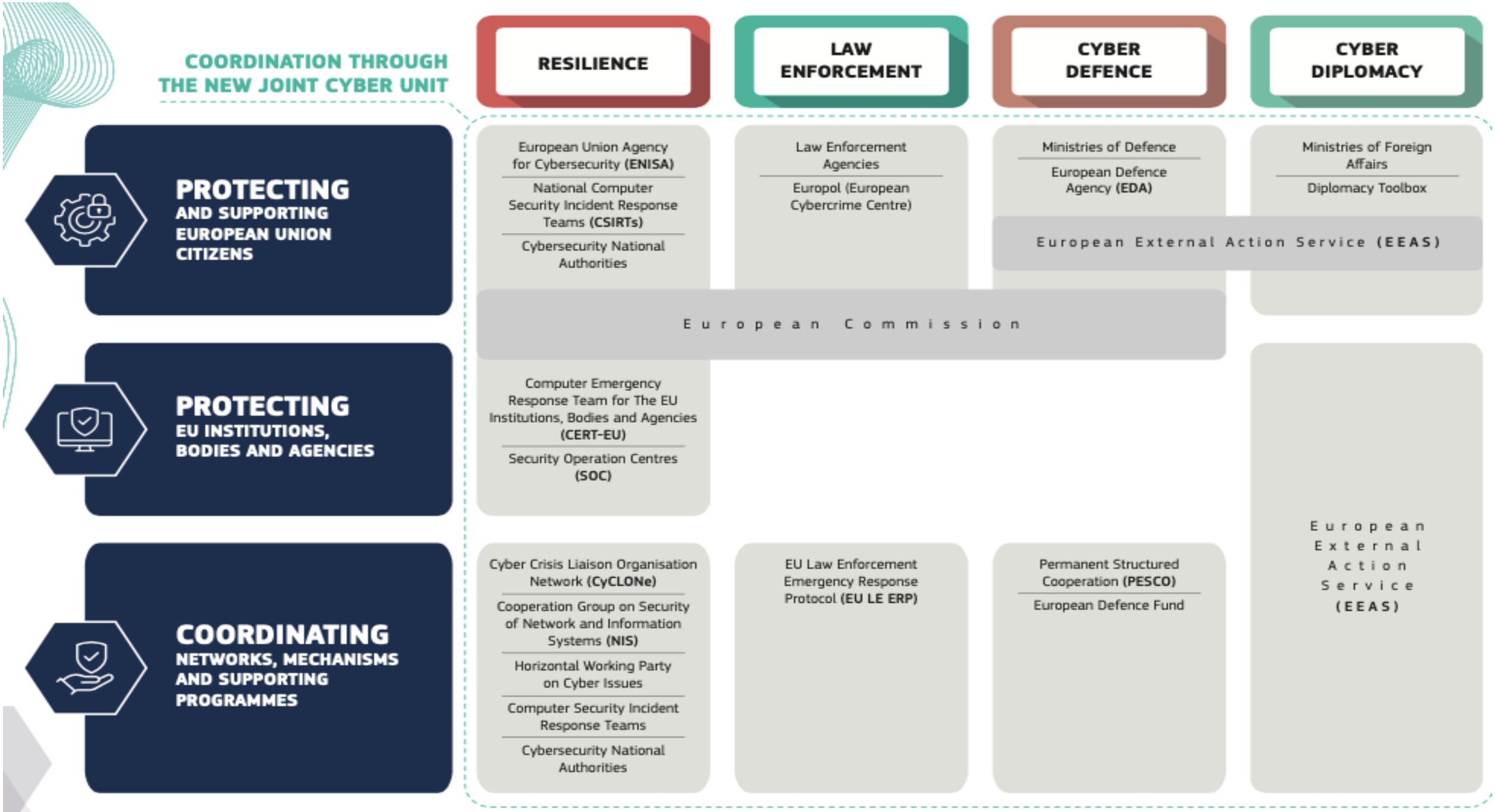
- **Cooperazione strutturata permanente (PESCO)**

Un quadro e un processo per approfondire la cooperazione in materia di difesa, anche in materia di cibersicurezza, tra gli Stati membri dell'UE che sono in grado e disposti a farlo.

- **Agenzia europea per la difesa**

Sostiene gli Stati membri nello sviluppo delle loro capacità di ciberdifesa, definite come la capacità di rilevare, resistere e riprendersi da qualsiasi attacco informatico; sostiene gli Stati membri nella definizione delle priorità a livello dell'UE per la ciberdifesa

sintesi dell'ecosistema della strategia europea di Cybersecurity


COORDINATION THROUGH THE NEW JOINT CYBER UNIT
RESILIENCE
LAW ENFORCEMENT
CYBER DEFENCE
CYBER DIPLOMACY
PROTECTING AND SUPPORTING EUROPEAN UNION CITIZENS
PROTECTING EU INSTITUTIONS, BODIES AND AGENCIES
COORDINATING NETWORKS, MECHANISMS AND SUPPORTING PROGRAMMES
European Union Agency for Cybersecurity (ENISA)
National Computer Security Incident Response Teams (CSIRTs)
Cybersecurity National Authorities
Law Enforcement Agencies
Europol (European Cybercrime Centre)
Ministries of Defence
European Defence Agency (EDA)
Ministries of Foreign Affairs
Diplomacy Toolbox
European External Action Service (EEAS)
European Commission
Computer Emergency Response Team for The EU Institutions, Bodies and Agencies (CERT-EU)
Security Operation Centres (SOC)
Cyber Crisis Liaison Organisation Network (CyCLONe)
Cooperation Group on Security of Network and Information Systems (NIS)
Horizontal Working Party on Cyber Issues
Computer Security Incident Response Teams
Cybersecurity National Authorities
EU Law Enforcement Emergency Response Protocol (EU LE ERP)
Permanent Structured Cooperation (PESCO)
European Defence Fund
European External Action Service (EEAS)

Strategia dell'UE per la cibersicurezza per il decennio digitale

https://digital-strategy.ec.europa.eu/en

GRAZIE PER LA VOSTRA ATTENZIONE!

Per informazioni
Vittorio.Calaprice@ec.europa.eu