



## Ciberdifesa: potenziata l'azione dell'UE contro le minacce informatiche

Bruxelles, 10 novembre 2022

Commissione e Alto rappresentante hanno presentato oggi la comunicazione congiunta sulla politica di ciberdifesa dell'UE e il piano d'azione sulla mobilità militare 2.0, per reagire al deterioramento della situazione della sicurezza risultante dall'aggressione russa nei confronti dell'Ucraina e per potenziare la capacità dell'Unione di proteggere la propria popolazione e le proprie infrastrutture.

Grazie alla nuova politica l'UE potenzierà la cooperazione e gli investimenti nella ciberdifesa per parare il numero sempre maggiore di ciberattacchi migliorando protezione, rilevamento, deterrenza e difesa.

Il ciberspazio non conosce confini. I recenti attacchi informatici alle reti energetiche, infrastrutture di trasporto e risorse spaziali evidenziano i rischi cui sono esposti i diversi attori, siano essi civili o militari. Ne consegue la necessità di intervenire più risolutamente per proteggere dalle minacce informatiche la popolazione e le forze armate, ma anche le missioni e operazioni civili e militari dell'UE.

La politica di ciberdifesa dell'UE mira a potenziare le capacità unionali nel settore e a rafforzare il coordinamento e la cooperazione tra le cibercomunità militari e civili (operatori della sfera civile, servizi di contrasto, servizi diplomatici, operatori della difesa). Migliorerà l'efficienza della gestione delle crisi informatiche nell'UE, di cui concorrerà a ridurre le dipendenze strategiche nel campo delle tecnologie informatiche critiche, rafforzando nel contempo la base industriale e tecnologica di difesa europea (EDTIB). Incentiverà la formazione dei talenti informatici e migliorerà la capacità di attrarli e trattenerli; intensificherà la cooperazione con i partner nel settore della ciberdifesa.

La politica di ciberdifesa dell'UE poggia su quattro pilastri che spaziano su un'ampia gamma di iniziative in grado di aiutare l'UE e gli Stati membri a:

- **intervenire insieme a rafforzamento della ciberdifesa dell'UE** - l'UE potenzierà i meccanismi di coordinamento tra attori nazionali e unionali nel settore della ciberdifesa, al fine di intensificare lo scambio di informazioni e la cooperazione fra le comunità militari e civili della ciberdifesa e sostenere maggiormente le missioni e le operazioni militari della PSDC;
- **mettere in sicurezza l'ecosistema di difesa dell'UE** - persino i componenti software non critici possono essere usati per attacchi informatici contro imprese o governi, anche nel settore della difesa. Occorre quindi lavorare ulteriormente alla normazione e certificazione della cibersicurezza per mettere al riparo i settori sia civile sia militare;
- **investire in capacità di ciberdifesa** - gli Stati membri devono aumentare considerevolmente gli investimenti in capacità militari di ciberdifesa moderne, collaborando tramite le piattaforme di cooperazione e i meccanismi di finanziamento disponibili a livello unionale, quali la cooperazione strutturata permanente (PESCO) e il Fondo europeo per la difesa, così come Orizzonte Europa e il programma Europa digitale;
- **stringere partenariati per superare le sfide comuni** - muovendo dai dialoghi in materia di sicurezza e difesa e nel settore cibernetico già esistenti con paesi partner, l'UE cercherà di stringere partenariati su misura nella ciberdifesa.

### Prossime tappe

La Commissione e l'Alto rappresentante -anche nella sua veste di capo dell'Agenzia europea per la difesa- presenteranno annualmente al Consiglio dell'Unione europea una relazione di monitoraggio e valutazione dello stato di attuazione delle azioni prospettate nella comunicazione congiunta sulla politica di ciberdifesa dell'UE. Gli Stati membri sono invitati a contribuire alla relazione comunicando l'andamento dell'attuazione che fa capo a misure nazionali o cooperative. In cooperazione con gli Stati membri potrebbe essere stabilito un piano di attuazione.

### Contesto

La strategia dell'UE in materia di cibersicurezza del 2020 ha rilevato la necessità di rivedere la

politica unionale di ciberdifesa. Anche la Presidente **von der Leyen**, nel [discorso sullo stato dell'Unione 2021](#), ha esortato a elaborare una politica europea della ciberdifesa, la quale costituisce anche uno degli obiettivi della [bussola strategica per la sicurezza e la difesa](#) approvata dal Consiglio a marzo di quest'anno. A maggio, nelle [conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica](#), gli Stati membri hanno invitato l'Alto rappresentante a presentare, insieme alla Commissione, una proposta ambiziosa per una politica dell'UE in materia di ciberdifesa nel 2022.

Insieme al pacchetto in materia di sicurezza e di difesa, la Commissione pubblica oggi anche la prima relazione sui progressi compiuti in merito al piano d'azione sulle sinergie tra l'industria civile, della difesa e dello spazio, disponibile [qui](#).

## Per ulteriori informazioni

[Comunicazione congiunta](#) sulla politica di ciberdifesa dell'UE

[Domande e risposte](#) sulla politica di ciberdifesa dell'UE

[Scheda informativa](#) sulla politica di ciberdifesa dell'UE

[Strategia dell'UE in materia di cibersicurezza](#) per il decennio digitale

[Scheda informativa](#) sulla nuova strategia dell'UE in materia di cibersicurezza

Discorso sullo [stato dell'Unione 2021](#)

[Bussola strategica](#) per la sicurezza e la difesa

[Conclusioni del Consiglio](#) sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica

[Comunicazione congiunta](#) sulle carenze di investimenti nel settore della difesa

Proposta di [legge sulla ciberresilienza](#)

[Scheda informativa](#) sulla cibersicurezza: azione esterna dell'UE

[Attività di ciberdifesa dell'Agenzia europea per la difesa](#)

[Unione europea della sicurezza](#)

[Per saperne di più sulla cibersicurezza](#)

[Per saperne di più sulla direttiva NIS](#)

IP/22/6642

Members of the college said:

La politica di ciberdifesa dell'UE dimostra che, abbinando gli strumenti civili e militari di cui disponiamo, possiamo essere più efficaci contro le minacce informatiche.

La guerra ha una nuova dimensione: la cibernetica. Per essere all'altezza delle sfide e delle minacce che incombono su di noi, abbiamo bisogno di forze armate europee moderne e interoperabili, dotate dei più moderni mezzi di ciberdifesa. La nuova politica di ciberdifesa dell'UE intensificherà la cooperazione tra gli attori unionali del settore e metterà a punto meccanismi che permettano di usare le capacità a livello di UE, compreso per le missioni e operazioni della PSDC. Potenzieremo così la nostra capacità di prevenzione, rilevamento, deterrenza e difesa dagli attacchi informatici, come ci chiede la bussola strategica.

Gli attacchi informatici sono spesso uno dei diversi elementi di una più ampia campagna ibrida, transfrontaliera per natura, e sono in grado di impattare sui sistemi e sulle infrastrutture civili e di difesa. Gli incidenti di cibersicurezza gravi possono comportare perturbazioni tali da impedire allo o agli Stati membri colpiti di gestirle autonomamente. L'Unione deve affermarsi con maggiore forza e credibilità come soggetto in grado di garantire sicurezza, anche nel ciberspazio. Su di noi incombono attacchi a carattere sempre più ibrido: una maggiore cooperazione tra le comunità degli operatori civili, di sicurezza e di difesa migliora quindi la nostra capacità di agire insieme a garanzia della sicurezza dell'UE.

Il riaffiorare di un conflitto ad alta intensità ci obbliga a rivedere l'approccio alla sicurezza dell'Europa: è il momento d'intensificare la cooperazione nella ciberdifesa per assicurare la capacità di protezione, rilevamento, deterrenza e difesa. Con una vasta gamma di nuove iniziative intendiamo operare incessantemente per il potenziamento delle capacità europee di ciberdifesa e intensificare la cooperazione tra le comunità che intervengono nella cibersicurezza. Una sicurezza più forte a dimensione unionale è il fondamento stesso della sovranità tecnologica dell'UE.

Contatti per la stampa:

[Peter STANO](#) (+32 2 295 45 53)

[Johannes BAHRKE](#) (+32 2 295 86 15)

[Adalbert JAHNZ](#) (+ 32 2 295 31 56)

[Sonya GOSPODINOVA](#) (+32 2 296 69 53)

Informazioni al pubblico: contattare [Europe Direct](#) telefonicamente allo [00 800 67 89 10 11](#) o per [e-mail](#)