Mercoledì 13 giugno 2018

P8_TA(2018)0258

Ciberdifesa

Risoluzione del Parlamento europeo del 13 giugno 2018 sulla ciberdifesa (2018/2004(INI))

(2020/C 28/06)

Il Parlamento europeo,

— visti il trattato sull'Unione europea (TUE) e il trattato sul funzionamento dell'Unione europea (TFUE),

— visto il documento dal titolo "Visione condivisa, azione comune: un'Europa più forte – Una strategia globale per la politica estera e di sicurezza dell'Unione europea", presentato dal vicepresidente della Commissione/alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza (VP/AR) il 28 giugno 2016,

— viste le conclusioni del Consiglio europeo del 20 dicembre 2013, del 26 giugno 2015, del 15 dicembre 2016, del 9 marzo 2017, del 22 giugno 2017, del 20 novembre 2017 e del 15 dicembre 2017,

— vista la comunicazione della Commissione del 7 giugno 2017 dal titolo "Documento di riflessione sul futuro della difesa europea" (COM(2017)0315),

— vista la comunicazione della Commissione del 7 giugno 2017 dal titolo "Istituzione del Fondo europeo per la difesa" (COM(2017)0295),

— vista la comunicazione della Commissione del 30 novembre 2016 sul piano d'azione europeo in materia di difesa (COM(2016)0950),

— vista la comunicazione congiunta della Commissione e dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza del 7 febbraio 2013 al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla Strategia dell'Unione europea per la cibersicurezza: Un ciberspazio aperto e sicuro (JOIN(2013)0001),

— visto il documento di lavoro dei servizi della Commissione del 13 settembre 2017 dal titolo "Valutazione della strategia dell'UE del 2013 per la cibersicurezza" (SWD(2017)0295),

— visto il quadro strategico dell'UE in materia di ciberdifesa, del 18 novembre 2014,

— viste le conclusioni del Consiglio del 10 febbraio 2015 sulla ciberdiplomazia,

— viste le conclusioni del Consiglio del 19 giugno 2017 su un quadro comune per una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica"),

— vista la comunicazione comune della Commissione alla Commissione e all'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza del 13 settembre 2017 al Parlamento europeo e al Consiglio dal titolo "Resilienza, deterrenza e difesa: Verso una cibersicurezza forte per l'UE (JOIN(2017)0450),

Mercoledì 13 giugno 2018

— visto il "Manuale di Tallinn 2.0 sul diritto internazionale applicabile alle operazioni cibernetiche" ([1]),

— vista la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione ([2]),

— visto il lavoro della Coalizione globale per la stabilità del ciberspazio,

— vista la comunicazione della Commissione, del 28 aprile 2015, intitolata "Agenda europea sulla sicurezza" (COM(2015)0185),

— vista la comunicazione congiunta della Commissione e dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza del 6 aprile 2016 al Parlamento europeo e al Consiglio, dal titolo "Quadro congiunto per contrastare le minacce ibride: una risposta dell'Unione europea" (JOIN(2016)0018),

— vista la sua risoluzione del 3 ottobre 2017 sulla lotta alla criminalità informatica ([3]),

— visti la dichiarazione congiunta dell'8 luglio 2016 dei Presidenti del Consiglio europeo e della Commissione e del Segretario generale della NATO, gli insiemi comuni di proposte per l'attuazione della dichiarazione congiunta approvati dai Consigli dell'UE e della NATO il 6 dicembre 2016 e il 5 dicembre 2017 e le relazioni sui progressi compiuti nella sua attuazione, del 14 giugno e del 5 dicembre 2017,

— vista la sua risoluzione del 22 novembre 2012 sulla sicurezza e la difesa informatica ([4]),

— vista la sua risoluzione del 22 novembre 2016 sull'Unione europea della difesa ([5]),

— vista la proposta della Commissione del 13 settembre 2017 riguardante unregolamento del Parlamento europeo e del Consiglio relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza") (COM(2017)0477),

— vista la sua risoluzione del 13 dicembre 2017 sulla relazione annuale relativa all'attuazione della politica estera di sicurezza comune (PESC) ([6]),

— vista la sua risoluzione del 13 dicembre 2017 sulla relazione annuale relativa all'attuazione della politica di sicurezza e di difesa comune (PSDC) ([7]),

— visto l'articolo 52 del suo regolamento,

— vista la relazione della commissione per gli affari esteri (A8-0189/2018),

A. considerando che le sfide, le minacce e gli attacchi informatici e ibridi costituiscono una notevole minaccia alla sicurezza, alla difesa, alla stabilità e alla competitività dell'UE, dei suoi Stati membri e dei suoi cittadini; che la ciberdifesa comprende chiaramente una dimensione sia militare, sia civile;

([1]) Cambridge University Press, febbraio 2017, ISBN 9781316822524, https://doi.org/10.1017/9781316822524.
([2]) GU L 194 del 19.7.2016, pag. 1.
([3]) Testi approvati, P8_TA(2017)0366.
([4]) GU C 419 del 16.12.2015, pag. 145.
([5]) Testi approvati, P8_TA(2016)0435.
([6]) Testi approvati, P8_TA(2017)0493.
([7]) Testi approvati, P8_TA(2017)0492.

B. considerando che l'UE e gli Stati membri si trovano a far fronte a una minaccia senza precedenti, sotto forma di ciberattacchi dettati da ragioni politiche e sponsorizzati dagli Stati, nonché a criminalità e terrorismo informatici;

C. considerando che il ciberspazio è ampiamente riconosciuto come il quinto settore operativo da parte delle forze armate, cosa che consente di sviluppare capacità di ciberdifesa; che l'opportunità di riconoscere il ciberspazio come il quinto settore di operazioni militari è oggetto di dibattito;

D. considerando che la clausola di difesa reciproca, di cui all'articolo 42, paragrafo 7 del TUE, prevede, in caso di un'aggressione armata nel territorio di uno Stato membro, un obbligo reciproco di prestargli aiuto e assistenza con tutti i mezzi in possesso; che ciò non pregiudica il carattere specifico della politica di sicurezza e di difesa di determinati Stati membri; che la clausola di solidarietà, di cui all'articolo 222 del TFUE, integra la clausola di difesa reciproca prevedendo che gli Stati membri dell'UE siano tenuti ad agire congiuntamente qualora uno Stato membro sia oggetto di un attacco terroristico o sia vittima di una calamità naturale o provocata dall'uomo; che la clausola di solidarietà comporta l'utilizzo di strutture sia civili che militari;

E. considerando che, se la ciberdifesa rimane una competenza centrale degli Stati membri, l'UE ha d'altronde un ruolo fondamentale da svolgere nel fornire una piattaforma per la cooperazione europea e nell'assicurare che le nuove iniziative siano, fin dall'inizio, strettamente coordinate a livello internazionale e all'interno dell'architettura della sicurezza transatlantica, per evitare divari e altre inefficienze che caratterizzano molti sforzi di difesa tradizionali; che è necessario fare di più, oltre a intensificare la cooperazione e il coordinamento; considerando che occorre garantire una prevenzione efficace potenziando la capacità dell'UE di individuare, difendere e scoraggiare; considerando che una difesa informatica e di dissuasione credibile è necessaria per conseguire un'efficace sicurezza informatica per l'UE, garantendo al contempo che i paesi che sono i meno preparati non diventino facile bersaglio di attacchi informatici, e che una capacità rilevante di difesa informatica dovrebbe essere un elemento necessario della PSDC e dello sviluppo dell'Unione europea della difesa; considerando la perenne scarsità di specialisti di difesa informatica altamente qualificati; che uno stretto coordinamento sulla protezione delle forze armate dai ciberattacchi è un elemento necessario per lo sviluppo di una PSDC effettiva;

F. considerando che gli Stati membri dell'UE sono spesso oggetto di attacchi informatici condotti da soggetti statali e non statali ostili e pericolosi, contro obiettivi civili o militari; considerando che l'attuale vulnerabilità è dovuta principalmente alla frammentazione delle strategie e delle capacità di difesa europea, cosa che consente alle agenzie di intelligence di sfruttare ripetutamente le vulnerabilità in materia di sicurezza dei sistemi informatici e delle reti, essenziali per la sicurezza europea; considerando che i governi degli Stati membri hanno spesso omesso di informare le parti interessate in tempo utile per consentire loro di far fronte alle vulnerabilità dei loro prodotti e servizi; considerando che tali attacchi necessitano di urgente rafforzamento e dello sviluppo di capacità offensive e difensive a livello civile e militare, al fine di evitare il possibile impatto economico e sociale di incidenti informatici;

G. considerando che nel ciberspazio la linea di demarcazione tra interferenza civile e militare diventa meno netta;

H. considerando che molti incidenti informatici sono causati dalla mancanza di resilienza e di solidità dell'infrastruttura della rete pubblica e privata, di banche dati scarsamente protette o insicure e ad altre lacune nell'infrastruttura critica informatizzata; che solo pochi Stati membri si assumono la responsabilità per la protezione delle rispettive reti e sistemi di informazione e dei dati associati, quale parte del proprio rispettivo dovere di diligenza, il che spiega la generale assenza di investimenti nella formazione e nella tecnologia di sicurezza all'avanguardia e nello sviluppo di linee guida adeguate;

I. considerando che il diritto alla privacy e il diritto alla protezione dei dati sono sanciti dalla Carta dei diritti fondamentali dell'UE e all'articolo 16 del TFUE e sono disciplinati dal regolamento generale dell'UE sulla protezione dei dati, entrato in vigore il 25 maggio 2018;

J. considerando che una politica del ciberspazio attiva ed efficace è in grado di dissuadere i nemici, di smantellarne le capacità e di anticiparne e demolirne le capacità di attacco;

Mercoledì 13 giugno 2018

K. considerando che diversi gruppi e organizzazioni terroristici utilizzano il ciberspazio quale strumento a basso costo per il reclutamento, la radicalizzazione e la diffusione della propaganda terroristica; che i gruppi terroristici, gli attori non statali e le reti criminali transnazionali utilizzano le operazioni informatiche per raccogliere fondi in modo anonimo, raccogliere informazioni e mettere a punto armi informatiche per realizzare campagne di ciberterrorismo, perturbare, danneggiare o distruggere infrastrutture critiche, o per attaccare sistemi finanziari e perseguire altre attività illegali che hanno conseguenze rilevanti per la sicurezza dei cittadini europei;

L. considerando che la deterrenza e la difesa informatica delle forze armate e delle infrastrutture critiche dell'Europa hanno assunto un ruolo fondamentale nei dibattiti sulla modernizzazione nel settore della difesa, gli sforzi di difesa comune dell'Europa, il futuro sviluppo delle forze armate e le loro operazioni e l'autonomia strategica dell'Unione europea;

M. considerando che diversi Stati membri hanno investito in misura sostanziale nella creazione di comandi informatici, dotati del personale necessario per far fronte a queste nuove sfide e per migliorare la loro resilienza informatica, ma occorre fare molto di più, dal momento che è sempre più difficile contrastare gli attacchi informatici a livello di Stato membro; considerando che i comandi informatici dei rispettivi Stati membri variano in funzione dei mandati offensivi e difensivi; che le altre strutture della difesa informatica variano notevolmente tra gli Stati membri e spesso sono frammentate; considerando che la difesa informatica e la deterrenza sono attività che possono essere meglio affrontate cooperando, a livello europeo e con i partner e gli alleati dell'Unione, dal momento che il loro ambito operativo non riconosce né confini nazionali né confini organizzativi; considerando che la sicurezza informatica e quella militare sono strettamente connesse e sono pertanto necessarie maggiori sinergie tra specialisti civili e militari; considerando che la notevole esperienza delle società private in questo settore solleva questioni di fondo circa la governance e la sicurezza, e circa la capacità degli Stati di difendere i propri cittadini;

N. considerando che è urgente rafforzare le capacità dell'UE nel campo della ciberdifesa, a causa della mancanza di una risposta sufficientemente rapida all'evoluzione della sicurezza informatica; che una risposta rapida e una preparazione adeguata sono elementi chiave per garantire la sicurezza in questo campo;

O. considerando che la cooperazione strutturata permanente (PESCO) e il Fondo europeo per la difesa (FES) sono iniziative nuove con il necessario margine per promuovere un ecosistema che possa fornire opportunità alle PMI e alle startup, e per agevolare i progetti di cooperazione nel settore della difesa informatica, e che entrambe contribuiranno a delineare il quadro normativo e istituzionale;

P. considerando che gli Stati membri partecipanti alla PESCO si sono impegnati a garantire che gli sforzi di cooperazione in materia di ciberdifesa, come la condivisione delle informazioni, la formazione e il sostegno operativo, continueranno a crescere;

Q. considerando che tra i diciassette progetti selezionati per la PESCO ve ne sono due in materia di ciberdifesa;

R. considerando che il FES deve sostenere la competitività globale e la capacità innovativa dell'industria europea della difesa, investendo in tecnologie digitali e informatiche, nonché favorire lo sviluppo di soluzioni intelligenti, offrendo alle PMI e alle startup opportunità per partecipare a tale sforzo;

S. considerando che l'Agenzia europea per la difesa (AED) ha avviato una serie di progetti per soddisfare la necessità degli Stati membri di sviluppare le loro capacità di ciberdifesa, compresi progetti in materia di istruzione e formazione, come la piattaforma di coordinamento delle esercitazioni e della formazione in materia di ciberdifesa (CD TEXP), il sostegno del settore privato alla messa in comune delle richieste di corsi di formazione ed esercitazioni in materia di ciberdifesa (DePoCyTE) e il progetto poligoni virtuali;

T. considerando che vi sono altri progetti dell'UE in corso sulla consapevolezza situazionale, l'individuazione di malware e la condivisione delle informazioni (the Malaware Information Sharing Platform (MISP) e il Multi-Agent System For Advanced persistent threat Detection (MASFAD));

U. considerando che le esigenze di sviluppo delle capacità e di formazione nel settore della ciberdifesa sono notevoli e crescenti e che esse sono soddisfatte nel modo più efficace cooperando a livello di UE e di NATO;

V. considerando che le missioni e le operazioni della PSDC, come tutti i moderni sforzi organizzativi, si basano profondamente su sistemi informatici funzionanti; che le minacce informatiche alle missioni e operazioni della PSDC possono esistere a diversi livelli che spaziano dal livello tattico (missioni e operazioni della PSDC) e operativo (reti dell'UE) all'infrastruttura informatica globale più ampia;

W. considerando che i sistemi di comando e controllo, lo scambio di informazioni e la logistica si avvalgono di infrastrutture informatiche classificate e non classificate, in particolare a livello tattico e operativo; che questi sistemi sono bersagli appetibili per operatori malintenzionati che cercano di attaccare le missioni; che i ciberattacchi possono avere ripercussioni significative sull'infrastruttura dell'Unione europea; considerando che i ciberattacchi contro, in particolare, le infrastrutture energetiche dell'UE potrebbero avere gravi conseguenze, e che esse devono pertanto essere protette;

X. considerando che è ben chiaro che la difesa informatica dovrebbe essere debitamente presa in considerazione in tutte le fasi del processo di pianificazione delle missioni e delle operazioni della PSDC, che essa richiede un monitoraggio costante, e che è necessario disporre di un'adeguata capacità di integrarlo pienamente nella pianificazione delle missioni e di continuare a fornire il necessario sostegno;

Y. considerando che la rete del Collegio europeo di sicurezza e difesa (ESDC) è l'unico fornitore europeo di formazione per le strutture, le missioni e le operazioni della PSDC; che, secondo i piani attuali, il suo ruolo nella messa in comune delle capacità europee di formazione nel settore informatico deve essere aumentato notevolmente;

Z. considerando che la dichiarazione del vertice di Varsavia della NATO, nel 2016, ha riconosciuto il ciberspazio come un settore di attività in cui la NATO deve difendersi efficacemente, come in realtà fa, in aria, su terra e in mare;

AA. considerando che l'UE e la NATO hanno contribuito a migliorare le capacità di difesa informatica degli Stati membri attraverso progetti di ricerca a duplice uso, coordinati dall'AED e dalla NATO, nonché migliorando la resilienza informatica della NATO attraverso il sostegno fornito dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA);

AB. considerando che nel 2014 la NATO ha stabilito che le operazioni di sicurezza informatica sono parte della sua difesa collettiva, e nel 2016 ha riconosciuto il ciberspazio come settore operativo su terra, in aria e in mare; che l'UE e la NATO sono partner complementari nello sviluppo della loro resilienza e capacità di difesa informatica; che la sicurezza e la difesa informatica sono già uno dei principali pilastri della cooperazione tra le due, e un settore critico in cui entrambe hanno capacità uniche; che nella dichiarazione congiunta UE-NATO, dell'8 luglio 2016, l'UE e la NATO hanno concordato un vasto programma di cooperazione; che quattro delle 42 proposte per una più stretta cooperazione riguardano la sicurezza e la difesa informatica, con ulteriori proposte volte a far fronte alle minacce ibride in senso più ampio; considerando che il 5 dicembre 2017 è stata aggiunta un'ulteriore proposta in merito alla sicurezza e alla difesa informatica;

AC. considerando che il gruppo di esperti governativi delle Nazioni Unite sulla sicurezza dell'informazione (UNGGE) ha concluso il suo ultimo ciclo di deliberazione; che, anche se esso non è stato in grado di pervenire a un consenso nel 2017, si applicano le relazioni del 2015 e del 2013, compreso il riconoscimento che il diritto internazionale vigente, in particolare la Carta delle Nazioni Unite, è applicabile ed è essenziale per il mantenimento della pace e della stabilità, per promuovere un contesto TIC aperto, sicuro, pacifico e accessibile;

AD. considerando che il quadro, lanciato di recente, per una risposta diplomatica comune dell'UE alle attività informatiche dolose, il cd. pacchetto di strumenti della diplomazia informatica dell'UE, inteso a sviluppare le capacità dell'UE e degli Stati membri per influenzare sul comportamento dei potenziali aggressori, prevede l'uso di misure proporzionate nell'ambito della PESC, comprese misure restrittive;

AE. considerando che diversi attori statali quali, tra gli altri, la Russia, la Cina e la Corea del Nord, ma anche attori non statali (compresi i gruppi di criminalità organizzata), ispirati, noleggiati o sponsorizzati da Stati e da agenzie di sicurezza o da società private – sono stati coinvolti in attività informatiche dolose nel perseguimento di obiettivi politici, economici o di sicurezza che includono attacchi alle infrastrutture critiche, lo spionaggio informatico e la sorveglianza di massa dei cittadini dell'UE, il favoreggiamento di campagne di disinformazione e di distribuzione di malware (WannaCry e NotPetya, ecc.), che limitano l'accesso a Internet e il funzionamento di sistemi di tecnologia dell'informazione; considerando che tali attività non tengono conto del diritto internazionale, lo violano e violano anche i diritti umani e i diritti fondamentali dell'UE, mettendo a repentaglio la democrazia, la sicurezza, l'ordine pubblico e l'autonomia strategica dell'UE, e dovrebbero quindi portare a una risposta comune dell'UE, come l'utilizzo del quadro di riferimento per una risposta diplomatica congiunta dell'UE, compreso il ricorso a misure restrittive previste per il pacchetto dell'UE in materia di diplomazia informatica, come ad esempio nel caso di imprese private, ammende e restrizioni di accesso al mercato interno;

AF. considerando che tali attacchi su larga scala contro le infrastrutture TIC hanno avuto luogo più volte nel passato, in particolare, in Estonia nel 2007, in Georgia nel 2008, e attualmente, quasi quotidianamente, in Ucraina; che le capacità informatiche offensive sono impiegate a un livello senza precedenti, anche contro gli Stati membri dell'UE e della NATO;

AG. considerando che le tecnologie della sicurezza informatica, sia in ambito civile che in ambito militare, sono tecnologie "a duplice uso", che offrono numerose opportunità per lo sviluppo di sinergie tra gli attori civili e militari in un certo numero di settori, quali la gestione della cifratura, della sicurezza e della vulnerabilità degli strumenti, nonché sistemi di rilevamento e prevenzione delle intrusioni;

AH. considerando che nei prossimi anni lo sviluppo delle tecnologie informatiche riguarderà nuovi settori quali l'intelligenza artificiale, l'internet degli oggetti, la robotica e i dispositivi mobili, e che tutti questi elementi possono anche avere implicazioni per la sicurezza del settore della difesa;

AI. considerando che i cibercomandi istituiti da vari Stati membri possono apportare un notevole contributo alla protezione delle infrastrutture civili fondamentali e che la conoscenza connessa alla ciberdifesa è spesso parimenti utile in ambito civile;

Sviluppo di capacità di ciberdifesa e deterrenza

1. sottolinea che, ai fini dello sviluppo dell'Unione europea della difesa, una politica comune di ciberdifesa e una notevole capacità di difesa informatica dovrebbero costituire elementi essenziali;

2. accoglie con favore l'iniziativa della Commissione di un pacchetto sulla sicurezza informatica per promuovere la resilienza, la deterrenza e la difesa informatica dell'UE;

3. ricorda che la ciberdifesa presenta sia una dimensione militare che una dimensione civile e che ciò significa che è necessario un approccio strategico integrato e una stretta cooperazione tra le parti interessate, militari e civili;

4. chiede uno sviluppo coerente delle capacità informatiche in tutte le istituzioni e gli organi dell'UE, nonché negli Stati membri, e che siano fornite le necessarie soluzioni politiche e pratiche per superare i restanti ostacoli di natura politica, legislativa e organizzativa per la cooperazione in materia di difesa informatica; ritiene che gli scambi e la cooperazione, regolari e rafforzati, tra i pertinenti portatori di interessi pubblici in materia di difesa informatica e a livello europeo e nazionale, siano elementi essenziali;

5. sottolinea con forza che, nel quadro dell'emergente Unione europea della difesa, le capacità di difesa informatica degli Stati membri dovrebbero essere in prima linea e, per quanto possibile, integrate sin dall'inizio per garantire la massima efficienza; esorta pertanto gli Stati membri a cooperare strettamente per lo sviluppo della propria ciberdifesa utilizzando una chiara tabella di marcia, alimentando in tal modo un processo coordinato dalla Commissione, dal Servizio europeo per l'azione esterna (SEAE) e dall'AED, al fine di una migliore razionalizzazione di strutture di ciberdifesa nei vari Stati membri, di attuare con urgenza misure a breve termine disponibili e di promuovere lo scambio di competenze; è del parere che sia opportuno sviluppare una rete europea sicura per le informazioni e le infrastrutture critiche; riconosce che capacità di attribuzione solide sono un elemento essenziale per assicurare una difesa e una deterrenza informatiche efficaci, e che una prevenzione effettiva richiede lo sviluppo di ulteriori sostanziali competenze tecnologiche; esorta gli Stati membri ad aumentare le risorse umane e finanziarie, in particolare il numero degli esperti di informatica forense, al fine di migliorare l'attribuzione degli attacchi informatici; sottolinea che tale cooperazione dovrebbe essere attuata anche mediante il rafforzamento dell'ENISA;

6. riconosce che molti Stati membri ritengono che il possesso di proprie capacità di ciberdifesa debba essere al centro della loro strategia di sicurezza nazionale e costituire un elemento essenziale della loro sovranità nazionale; sottolinea, tuttavia, che a causa del carattere "senza frontiere" del ciberspazio, la portata e le conoscenze necessarie di forze veramente globali ed efficaci, in grado di garantire l'obiettivo dell'autonomia strategica dell'UE nel ciberspazio, fuori dalla portata di qualsiasi singolo Stato membro e richiedono, quindi, una risposta rafforzata e coordinata da parte di tutti gli Stati membri, a livello di UE; osserva, in questo contesto, che l'UE e i suoi Stati membri si trovano ad affrontare pressioni causate dal poco tempo a disposizione per sviluppare dette forze e che essi devono agire immediatamente; constata che, a seguito di iniziative dell'UE quali il mercato unico digitale, l'Unione si trova nella posizione ideale per assumere un ruolo guida nell'elaborazione di strategie di difesa informatica a livello europeo; ribadisce che lo sviluppo della ciberdifesa a livello di UE deve migliorare la capacità dell'Unione di proteggere se stessa; accoglie con favore, a tale riguardo, il mandato permanente proposto per l'ENISA, e il suo rafforzamento;

7. sollecita gli Stati membri, in tale contesto, a fare il miglior uso possibile del quadro fornito dalla PESCO e dal FES per proporre progetti di cooperazione;

8. prende atto dell'intensa attività svolta dall'UE e dai suoi Stati membri in materia di difesa informatica; prende in particolare atto dei progetti dell'AED in materia di poligoni virtuali, dell'Agenda di ricerca strategica sulla ciberdifesa e dello sviluppo della consapevolezza dei quartieri generali della situazione informatica utilizzabile;

9. accoglie con favore i due progetti informatici da lanciare nel quadro della PESCO, vale a dire la piattaforma per la condivisione delle informazioni in materia di minaccia informatica e di risposta agli incidenti e i gruppi di risposta rapida agli incidenti informatici e di reciproca assistenza in materia di sicurezza informatica; sottolinea che questi due progetti si concentrano su una politica di difesa informatica che si basa sulla condivisione di informazioni sulle minacce informatiche attraverso una piattaforma che consente agli Stati membri di creare gruppi di reazione rapida agli incidenti informatici (Cyber CRRT), nonché di aiutarsi a vicenda al fine di garantire un più alto livello di resilienza informatica e di individuare, riconoscere e mitigare congiuntamente le minacce informatiche; invita la Commissione e gli Stati membri a fare riferimento a progetti della PESCO basati sui CRRT nazionali e sull'assistenza reciproca in materia di cibersicurezza, istituendo un CRRT europeo incaricato di coordinare, individuare e contrastare le minacce informatiche collettive, a sostegno degli sforzi prodigati dagli Stati membri partecipanti;

10. osserva che la capacità europea di sviluppare progetti di ciberdifesa dipende dalla padronanza delle tecnologie, delle attrezzature, dei servizi e dei dati e dal relativo trattamento, nonché dal fatto che essa deve fondarsi su una base di attori industriali fidati;

11. ricorda che uno degli obiettivi degli sforzi volti a migliorare l'omogeneità dei sistemi di comando è quello di garantire che le risorse di comando disponibili siano interoperabili con quelle dei paesi della NATO non appartenenti all'UE, come pure con quelle dei partner occasionali, e a garantire un agevole scambio di informazioni, al fine di accelerare il processo decisionale e di mantenere il controllo della rete di informazioni in un contesto di rischio informatico;

12. raccomanda di trovare i modi per integrare i progetti di "difesa intelligente" della NATO, ad esempio lo sviluppo della capacità multinazionale di ciberdifesa, la piattaforma per lo scambio di informazioni sui malware (MISP) e l'istruzione e la formazione multinazionali in materia di ciberdifesa (MNCDE&T);

13. riconosce i progressi conseguiti in settori quali le nanotecnologie, l'intelligenza artificiale, i big data, i rifiuti elettronici e la robotica avanzata; esorta gli Stati membri e l'UE a dedicare particolare attenzione all'eventuale sfruttamento di questi settori da parte di attori statali ostili e di gruppi della criminalità organizzata; chiede la messa a punto di programmi di formazione e lo sviluppo di capacità, volti a proteggere contro regimi criminali sofisticati emergenti, quali frodi d'identità complesse e contraffazione di beni;

14. sottolinea la necessità di maggiore chiarezza terminologica in merito alla sicurezza nel ciberspazio, nonché di un approccio globale e integrato e di sforzi congiunti per contrastare le minacce informatiche e ibride e per individuare ed eliminare le "zone franche" online per le attività estremiste e criminali, rafforzando e aumentando la condivisione di informazioni tra l'UE e le sue agenzie, come Europol, Eurojust, AED ed ENISA;

15. sottolinea il ruolo crescente dell'intelligenza artificiale nei reati informatici e nella difesa; esorta l'UE e gli Stati membri a prestare particolare attenzione a questo settore, sia nell'ambito della ricerca che in quello dello sviluppo pratico, delle loro capacità di difesa informatica;

16. sottolinea fermamente che insieme alla diffusione di droni, armati o meno, dovrebbero essere adottate misure aggiuntive per ridurre le loro potenziali vulnerabilità informatiche;

Ciberdifesa di missioni e di operazioni della PSDC

17. sottolinea che la ciberdifesa dovrebbe essere considerata un compito operativo per le missioni e le operazioni della PSDC e dovrebbe essere inserita in tutti i processi di pianificazione della PSDC per garantire che la cibersicurezza sia costantemente considerata, in tutto il processo di pianificazione, così da ridurre le lacune in termini di vulnerabilità informatiche;

18. riconosce che la pianificazione di una missione, o di un'operazione della PSDC di successo, richiede notevoli competenze in materia di ciberdifesa e infrastrutture nonché reti informatiche molto sicure, sia a livello di quartier generale operativo che nell'ambito della missione stessa, per poter procedere a un'approfondita valutazione della minaccia e fornire un'adeguata protezione nel settore; invita il SEAE e gli Stati membri che mettono a disposizione i quartieri generali per le operazioni della PSDC a rafforzare le competenze in materia di difesa informatica, fornite alle missioni e alle operazioni dell'UE; osserva che vi è un limite al grado di efficacia di ogni missione della PSDC preparata per proteggersi dagli attacchi informatici;

19. sottolinea che la pianificazione di tutte le missioni e operazioni della PSDC deve essere accompagnata da una valutazione approfondita dello scenario delle minacce informatiche; osserva che la tassonomia delle minacce elaborata dall'ENISA offre un modello idoneo per tale valutazione; raccomanda di creare una capacità di valutazione della resilienza informatica dei quartieri generali della PSDC;

20. riconosce, in particolare, l'importanza di mantenere al minimo necessario le impronte informatiche e le superfici di attacco delle missioni e delle operazioni della PSDC; esorta i pianificatori coinvolti a tenerne conto sin dall'inizio del processo di pianificazione;

21. riconosce l'analisi delle esigenze di formazione dell'AED, che ha riscontrato importanti carenze in termini di capacità e competenze in materia di ciberdifesa tra i responsabili decisionali, non solo negli Stati membri, e accoglie con favore le iniziative dell'AED sui corsi per decisori di alto livello all'interno degli Stati membri, a sostegno della pianificazione delle missioni e delle operazioni della PSDC;

Istruzione e formazione in materia di ciberdifesa

22. osserva che la razionalizzazione del panorama dell'istruzione e formazione in materia di ciberdifesa dell'UE attenuerebbe notevolmente le minacce e invita l'UE e gli Stati membri ad aumentare la loro cooperazione nell'ambito dell'istruzione, della formazione e delle esercitazioni;

23. sostiene fortemente il programma Erasmus militare e altre iniziative comuni di formazione e scambio mirate a migliorare l'interoperabilità delle forze armate degli Stati membri e lo sviluppo di una cultura strategica comune attraverso maggiori scambi di giovane personale militare, tenendo presente che tale interoperabilità è necessaria tra tutti gli Stati membri e gli alleati della NATO; ritiene, tuttavia, che gli scambi per la formazione e l'istruzione nel settore della ciberdifesa dovrebbero andare oltre tale iniziativa e comprendere personale militare di tutte le età e di tutti i livelli così come studenti di tutti i centri di studio accademici sulla cibersicurezza;

24. sottolinea la necessità di un maggior numero di esperti nel settore della ciberdifesa; invita gli Stati membri a facilitare la cooperazione tra le istituzioni accademiche civili e le accademie militari per colmare questa carenza, al fine di creare maggiori possibilità nel campo dell'istruzione e della formazione in materia di ciberdifesa, e a destinare maggiori risorse alla formazione operativa specializzata in ambito informatico, anche in materia di intelligenza artificiale; invita le accademie militari a integrare l'educazione alla ciberdifesa nei programmi di studio, contribuendo in tal modo ad aumentare la riserva di talenti informatici disponibile per le esigenze delle missioni PSDC;

25. invita tutti gli Stati membri a informare, sensibilizzare e consigliare in modo sufficiente e proattivo le imprese, le scuole e i cittadini in merito alla cibersicurezza e alle principali minacce digitali; accoglie con favore, a tale riguardo, le guide informatiche quale strumento per orientare i cittadini e le organizzazioni verso una migliore strategia in materia di cibersicurezza, rafforzare la conoscenza in tale ambito e migliorare la resilienza informatica in vari settori;

26. osserva che, vista la necessità di personale più specializzato, gli Stati membri non dovrebbero impegnarsi unicamente ad assumere personale competente delle forze armate, bensì anche a mantenere gli esperti necessari;

27. accoglie con favore l'attuazione, da parte di undici Stati membri (Austria, Belgio, Germania, Estonia, Grecia, Finlandia, Irlanda, Lettonia, Paesi Bassi, Portogallo e Svezia), del progetto Cyber Ranges Federation, primo di quattro progetti di ciberdifesa avviati nel contesto dell'agenda dell'AED di messa in comune e condivisione; esorta gli altri Stati membri ad aderire a tale iniziativa; invita gli Stati membri a promuovere una maggiore disponibilità reciproca di formazione in materia di ciberdifesa e cibersicurezza; osserva a tale riguardo che è opportuno anche tenere conto del ruolo dell'ENISA e delle sue competenze;

28. ritiene che siffatte iniziative contribuiscano a migliorare la qualità dell'istruzione in materia di ciberdifesa a livello di UE, in particolare attraverso la creazione di piattaforme tecniche di più ampia portata e di una comunità di esperti dell'UE; ritiene che le forze armate europee possano diventare più interessanti fornendo una formazione globale in materia di ciberdifesa per attrarre e mantenere il talento informatico; sottolinea la necessità di individuare i punti deboli nei sistemi informatici sia degli Stati membri che delle istituzioni dell'UE; riconosce che l'errore umano è uno dei punti deboli individuati più di frequente nei sistemi di cibersicurezza e chiede pertanto corsi di formazione regolari per il personale sia militare che civile che lavora per le istituzioni dell'UE;

29. invita l'AED a lanciare la piattaforma di istruzione, formazione e coordinamento delle esercitazioni (CD TEXP) per sostenere la Cyber Ranges Federation quanto prima, focalizzando l'attenzione sul rafforzamento della cooperazione riguardo ai requisiti armonizzati, sulla promozione delle innovazioni nell'ambito della ricerca e della tecnologia in materia di ciberdifesa e sull'assistenza collettiva ai paesi terzi nel consolidamento delle loro capacità di creare resilienza nella ciberdifesa; invita la Commissione e gli Stati membri a integrare tali iniziative con un apposito centro europeo di eccellenza per la formazione in materia di ciberdifesa per fornire formazione specializzata alle reclute più promettenti, a sostegno della formazione informatica degli Stati membri partecipanti;

30. accoglie con favore la creazione, nell'ambito dell'AESD, della piattaforma di valutazione e di istruzione, formazione ed esercitazioni in materia di ciberdifesa (ETEE), nella prospettiva di migliorare le opportunità di formazione e istruzione all'interno degli Stati membri;

31. incoraggia maggiori scambi in materia di consapevolezza situazionale mediante esercitazioni informatiche di simulazione e il coordinamento dei rispettivi sforzi di sviluppo delle capacità al fine di conseguire maggiore interoperabilità e migliore prevenzione degli attacchi futuri nonché migliorare la risposta agli stessi; chiede che tali progetti siano condotti in collaborazione con gli alleati della NATO, le forze armate degli Stati membri dell'UE e altri partner con vasta esperienza nella lotta contro gli attacchi informatici, al fine di sviluppare prontezza operativa e procedure e norme comuni per affrontare in modo globale le diverse minacce informatiche; accoglie con favore, a tale riguardo, la partecipazione dell'UE alle esercitazioni informatiche, ad esempio l'esercitazione informatica in materia di offesa e difesa (CODE);

32. ricorda che un ciberspazio resiliente richiede un'igiene informatica impeccabile; invita tutte le parti interessate pubbliche e private a condurre corsi di formazione periodici sull'igiene informatica per tutti i membri del personale;

33. raccomanda l'intensificazione dello scambio di competenze ed esperienze tra forze armate, forze di polizia e altri organismi statali negli Stati membri coinvolti attivamente nella lotta contro le minacce informatiche;

Cooperazione tra l'UE e la NATO in materia di ciberdifesa

34. ribadisce che, in ragione dei valori e degli interessi strategici che condividono, l'UE e la NATO hanno una responsabilità e una capacità particolari nell'affrontare le crescenti sfide alla cibersicurezza e alla ciberdifesa in modo più efficace e in stretta collaborazione, cercando eventuali complementarità, evitando duplicazioni e riconoscendo le rispettive responsabilità;

35. invita il Consiglio, nell'ambito della collaborazione con altre istituzioni e strutture competenti dell'UE, a prendere in considerazione modalità per fornire al più presto un sostegno a livello di Unione per integrare il settore informatico nelle dottrine militari degli Stati membri, in maniera armonizzata e in stretta cooperazione con la NATO;

36. chiede l'attuazione delle misure già concordate; invita a individuare nuove iniziative volte a promuovere la cooperazione tra l'UE e la NATO, tenendo conto inoltre della possibilità di cooperare nell'ambito del Centro di eccellenza per la ciberdifesa cooperativa della NATO (CCD COE) e dell'Accademia delle comunicazioni e dell'informazione della NATO (NCI), che mirano ad aumentare le capacità di formazione in materia di ciberdifesa nei sistemi informatici e cibernetici, per quanto riguarda sia il software che l'hardware; osserva che ciò potrebbe includere un dialogo con la NATO sulla possibilità che l'UE aderisca al CCD COE al fine di aumentare la complementarità e la collaborazione; accoglie con favore la recente creazione del Centro europeo di eccellenza per la lotta contro le minacce ibride; esorta tutte le istituzioni competenti e gli alleati a discutere periodicamente delle loro attività al fine di evitare sovrapposizioni e incoraggiare un approccio coordinato alla ciberdifesa; ritiene fondamentale stimolare, sulla base della fiducia reciproca, lo scambio di informazioni sulle minacce informatiche tra gli Stati membri e con la NATO;

37. è convinto che nell'ambito della ciberdifesa sia importante e utile una maggiore cooperazione tra l'UE e la NATO per prevenire, rilevare e dissuadere i ciberattacchi; invita pertanto le due organizzazioni a intensificare la cooperazione e il coordinamento operativi e ad ampliare i loro sforzi comuni per creare capacità, in particolare sotto forma di esercitazioni e formazione congiunta per il personale civile e militare preposto alla ciberdifesa e attraverso la partecipazione degli Stati membri a progetti della NATO di difesa intelligente; ritiene fondamentale che l'UE e la NATO intensifichino la condivisione di informazioni al fine di consentire l'attribuzione formale dei ciberattacchi e quindi l'imposizione di sanzioni restrittive ai responsabili; esorta entrambe le organizzazioni a collaborare più strettamente anche sugli aspetti informatici della gestione delle crisi;

38. accoglie con favore lo scambio di concetti per integrare i requisiti e le norme di ciberdifesa nella pianificazione e nello svolgimento di missioni e operazioni nell'intento di promuovere l'interoperabilità ed esprime l'auspicio che ciò sia seguito da una collaborazione più operativa per garantire l'aspetto della ciberdifesa delle rispettive missioni e la sincronizzazione degli approcci operativi;

39. accoglie con favore l'accordo tra la Squadra di pronto intervento informatico dell'UE (CERT-UE) e la Capacità di reazione della NATO in caso di incidente informatico (NCIRC), volto ad agevolare lo scambio di informazioni, il supporto logistico, le valutazioni delle minacce condivise, l'assunzione di personale e la condivisione delle migliori pratiche, per assicurare la capacità rispondere alle minacce in tempo reale; sottolinea che è importante promuovere gli scambi di informazioni tra la CERT-EU e la NCIRC e adoperarsi per aumentare il livello di fiducia; ritiene che le informazioni detenute dalla CERT-UE possano probabilmente essere utili alla ricerca in materia di ciberdifesa e alla NATO e che tali informazioni dovrebbero pertanto essere condivise, purché sia garantita la piena conformità alla legislazione dell'UE sulla protezione dei dati;

40. accoglie con favore la cooperazione tra le due organizzazioni in materia di esercitazioni di ciberdifesa; prende atto della partecipazione dei rappresentanti dell'UE all'esercizio annuale della Cyber Coalition; riconosce il progresso che rappresenta la partecipazione dell'UE all'esercizio 2017 di gestione delle crisi della NATO, nel quadro delle esercitazioni parallele e coordinate (PACE 17), e accoglie con favore, in particolare, l'inclusione di una componente di ciberdifesa; esorta entrambe le organizzazioni a intensificare tali sforzi;

41. esorta l'UE e la NATO a organizzare regolarmente esercitazioni a livello strategico con la partecipazione dei massimi dirigenti politici di entrambe le organizzazioni; accoglie con favore, a tale riguardo, l'esercitazione estone UE CYBRID 2017 nel cui ambito il Segretario generale della NATO per la prima volta ha partecipato a un'esercitazione dell'UE;

42. osserva che vi è un ampio margine per un programma di cooperazione più ambizioso e concreto in materia di ciberdifesa che vada al di là del livello concettuale di cooperazione nell'ambito di specifiche operazioni; esorta entrambe le organizzazioni ad applicare, concretamente ed efficacemente, tutto ciò che già esiste e a presentare proposte più ambiziose per il prossimo esame dell'attuazione della dichiarazione congiunta;

43. accoglie con favore il partenariato informatico della NATO con l'industria (NICP), istituito nel 2014, e chiede che l'UE si impegni in attività di cooperazione di tale partenariato al fine di collegare lo sforzo di cooperazione NATO-UE con quello dei leader del settore specializzati in cibertecnologie, con l'obiettivo di promuovere la cibersicurezza attraverso una collaborazione continua, concentrandosi in particolare su: formazione, esercitazioni e istruzione dei rappresentanti della NATO, dell'UE e dell'industria, inclusione dell'UE e dell'industria nei progetti di difesa intelligente della NATO, condivisione collaborativa delle informazioni e delle migliori pratiche per la preparazione e il recupero tra la NATO, l'UE e l'industria, prosecuzione dello sviluppo congiunto di capacità di ciberdifesa e risposte collaborative in caso di incidenti informatici, ove e quando opportuno;

44. prende atto del lavoro in corso sulla proposta di regolamento che modifica il regolamento (UE) n. 526/2013 relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che stabilisce un quadro europeo per la certificazione della sicurezza e l'etichettatura delle TIC; invita l'ENISA a firmare un accordo con la NATO per aumentare la loro cooperazione pratica, ivi compresa la condivisione di informazioni e la partecipazione alle esercitazioni di ciberdifesa;

Norme internazionali applicabili al ciberspazio

45. chiede l'integrazione delle capacità di ciberdifesa nella PESC e nell'azione esterna dell'UE e dei suoi Stati membri quale compito trasversale e chiede un più stretto coordinamento in materia di ciberdifesa tra gli Stati membri, le istituzioni dell'UE, la NATO, le Nazioni Unite, gli Stati Uniti e altri partner strategici, in particolare per quanto riguarda le regole, le norme e le misure di attuazione nel ciberspazio;

46. si rammarica del fatto che, dopo vari mesi di negoziati, il gruppo di esperti governativi delle Nazioni Unite (UNGGE) 2016-2017 non sia stato in grado di elaborare una nuova relazione di consenso; ricorda che, come riconosciuto nella relazione del 2013, il diritto internazionale vigente e in particolare la Carta delle Nazioni Unite – che vieta la minaccia o l'uso della forza contro l'indipendenza politica di qualsiasi Stato, comprese le operazioni cibernetiche coercitive volte a perturbare l'infrastruttura tecnica essenziale per lo svolgimento di procedure partecipative ufficiali, incluse le elezioni, in un altro Stato – si applicano e dovrebbero essere applicate nel ciberspazio; rileva che la relazione del 2015 dell'UNGGE elenca una serie di norme di comportamento responsabile degli Stati, tra cui il divieto imposto a questi ultimi di effettuare e sostenere consapevolmente attività informatiche contrarie ai loro obblighi ai sensi delle norme internazionali; invita l'UE ad assumere un ruolo di primo piano nei dibattiti in corso e futuri sulle norme internazionali nel ciberspazio e sulla loro attuazione;

47. prende atto dell'importanza del Manuale di Tallinn 2.0 in quanto base per un dibattito e un'analisi del modo in cui il diritto internazionale vigente possa essere applicato al ciberspazio; invita gli Stati membri ad avviare l'analisi e l'applicazione di quanto affermato dagli esperti nel manuale di Tallinn e a concordare ulteriori norme volontarie di comportamento internazionale; osserva, in particolare, che un eventuale utilizzo offensivo delle capacità informatiche dovrebbe basarsi sul diritto internazionale;

48. conferma il suo pieno impegno a favore di un ciberspazio aperto, libero, stabile e sicuro, che rispetti i valori fondamentali della democrazia, dei diritti umani e dello Stato di diritto e dove le controversie internazionali siano composte con mezzi pacifici sulla base della Carta delle Nazioni Unite e dei principi di diritto internazionale; invita gli Stati membri a promuovere un'ulteriore attuazione dell'approccio comune e globale dell'UE nei confronti della ciberdiplomazia e delle norme informatiche vigenti e a redigere, unitamente alla NATO, criteri e definizioni a livello dell'UE di ciò che costituisce un ciberattacco in modo da migliorare la capacità dell'UE di giungere rapidamente a una posizione comune a seguito di un atto illecito a livello internazionale sotto forma di ciberattacco; sostiene con forza l'attuazione delle norme volontarie e non vincolanti di comportamento responsabile dello Stato nel ciberspazio contenute nella relazione UNGGE 2015, che comprendono il rispetto della vita privata e dei diritti fondamentali dei cittadini e la creazione di misure regionali volte a rafforzare la fiducia; sostiene, in questo contesto, il lavoro della Coalizione globale per la stabilità del ciberspazio per elaborare proposte di norme e politiche volte a rafforzare la sicurezza e la stabilità internazionali e orientare il comportamento responsabile degli attori statali e non statali nel ciberspazio; approva la proposta secondo cui gli attori statali e non statali non devono svolgere o consentire consapevolmente un'attività che danneggi in maniera intenzionale e sostanziale la disponibilità o l'integrità generale del nucleo pubblico di Internet, e pertanto la stabilità del ciberspazio;

49. riconosce che la maggior parte delle infrastrutture tecnologiche è detenuta o gestita dal settore privato e che è pertanto essenziale una stretta cooperazione, consultazione e inclusione dei gruppi del settore privato e della società civile mediante il dialogo multilaterale per garantire un ciberspazio aperto, libero, stabile e sicuro;

Mercoledì 13 giugno 2018

50. riconosce che, a causa delle difficoltà connesse all'applicazione, gli accordi bilaterali tra Stati membri non sempre producono i risultati attesi; ritiene pertanto che la creazione di coalizioni all'interno di gruppi di paesi che condividono gli stessi principi, intenzionati a creare consenso, costituisca un modo efficace per integrare gli sforzi delle molteplici parti interessate; sottolinea l'importanza del ruolo che le autorità locali devono svolgere, nel processo di innovazione tecnologica e di condivisione dei dati per intensificare la lotta contro la criminalità e le attività terroristiche;

51. accoglie con favore l'adozione da parte del Consiglio del quadro per le risposte diplomatiche comuni dell'UE alle attività informatiche malevole, il cosiddetto pacchetto di strumenti della diplomazia informatica dell'UE; sostiene la possibilità che l'UE adotti misure restrittive contro gli avversari che attaccano i suoi Stati membri nel ciberspazio, ivi compresa l'imposizione di sanzioni;

52. invita inoltre ad adottare un chiaro approccio proattivo alla cibersicurezza e alla ciberdifesa e a rafforzare la ciberdiplomazia dell'UE, quale compito trasversale nella sua politica estera, e le capacità e gli strumenti di cui dispone in vari settori, così da consolidare efficacemente le norme e i valori dell'UE e spianare la strada per raggiungere un consenso sulle regole, sulle norme e sulle misure di esecuzione nel ciberspazio a livello mondiale; osserva che la costruzione della resilienza informatica nei paesi terzi contribuisce alla pace e alla sicurezza internazionali e, in ultima analisi, garantisce più sicurezza ai cittadini europei;

53. ritiene che i ciberattacchi come NotPetya e WannaCry siano diretti da uno Stato o condotti con la consapevolezza e l'approvazione di uno Stato; osserva che tali ciberattacchi, che causano danni economici gravi e duraturi e costituiscono una minaccia per la vita, sono chiare violazioni del diritto internazionale e delle norme giuridiche; ritiene pertanto che NotPetya e WannaCry rappresentino violazioni del diritto internazionale commesse rispettivamente dalla Federazione russa e dalla Corea del Nord, e che i due paesi dovrebbero affrontare risposte commisurate e adeguate da parte dell'UE e della NATO;

54. chiede che il Centro per la lotta alla criminalità informatica di Europol diventi un punto focale per le divisioni incaricate dell'applicazione della legge e le agenzie governative che si occupano di cibercriminalità, la cui responsabilità primaria sarebbe quella di gestire la difesa sia dei domini .eu che delle infrastrutture critiche delle reti dell'UE durante un attacco; sottolinea che tale punto focale dovrebbe essere inoltre incaricato di scambiare informazioni e fornire assistenza agli Stati membri;

55. sottolinea l'importanza dell'elaborazione di norme in materia di vita privata e sicurezza, crittografia, incitamento all'odio, disinformazione e minacce terroristiche;

56. raccomanda che ciascuno Stato membro dell'UE si assuma l'obbligo di assistere qualsiasi altro Stato membro vittima di un ciberattacco e di garantire la responsabilità informatica nazionale in stretta cooperazione con la NATO;

Cooperazione civile-militare

57. invita tutte le parti interessate a rafforzare i partenariati per il trasferimento di conoscenze, ad attuare modelli commerciali adeguati e a sviluppare la fiducia tra le imprese e gli utilizzatori finali nella sfera civile e nel settore della difesa, nonché a migliorare il trasferimento delle conoscenze accademiche concretizzandole in soluzioni pratiche, al fine di creare sinergie e trasferire soluzioni fra i mercati civile e militare – essenzialmente un mercato unico europeo per la cibersicurezza e i prodotti per la cibersicurezza – in base a procedure trasparenti e nel rispetto del diritto internazionale e dell'UE, nell'ottica di tutelare e rafforzare l'autonomia strategica dell'UE; osserva il ruolo centrale svolto dalle imprese private operanti nel settore della cibersicurezza nell'allarme rapido e nell'attribuzione dei ciberattacchi;

58. ribadisce con forza l'importanza delle attività di ricerca e sviluppo, in particolare alla luce dei requisiti di sicurezza ad alto livello nel mercato della difesa; esorta l'UE e gli Stati membri ad attribuire un maggiore sostegno pratico all'industria europea della cibersicurezza e ad altri attori economici pertinenti, a ridurre gli oneri burocratici, in particolare per le PMI e le start-up, fonti principali di soluzioni innovative nel settore della ciberdifesa, e a promuovere una più stretta cooperazione con gli istituti di ricerca universitaria e i grandi operatori, al fine di ridurre la dipendenza da prodotti della cibersicurezza provenienti da fonti esterne e di creare una filiera strategica all'interno dell'UE per rafforzare l'autonomia strategica di quest'ultima; rileva, in tale contesto, l'importante contributo che può essere fornito dal FED e da altri strumenti nell'ambito del Quadro finanziario pluriennale (QFP);

59. incoraggia la Commissione a integrare elementi della ciberdifesa nella rete dei centri europei di ricerca e competenza in materia di cibersicurezza, anche al fine di fornire risorse sufficienti alle capacità e alle tecnologie informatiche a duplice uso nell'ambito del prossimo QFP;

60. rileva che la protezione dei beni pubblici e delle altre infrastrutture critiche civili, in particolare i sistemi di informazione e i dati associati, è un compito di difesa essenziale per gli Stati membri, e in particolare per le autorità responsabili della sicurezza dei sistemi di informazione, e che dovrebbe rientrare nelle competenze delle strutture nazionali di ciberdifesa o di suddette autorità; sottolinea che ciò richiederà un buon livello di fiducia nonché la cooperazione più stretta possibile tra gli attori militari, le agenzie preposte alla ciberdifesa e i settori interessati, il che potrà essere realizzato soltanto definendo chiaramente compiti, ruoli e responsabilità degli attori civili e militari, ed esorta tutte le parti coinvolte a tenerne conto nei loro processi di pianificazione; chiede una maggiore cooperazione transfrontaliera, nel pieno rispetto della legislazione dell'UE sulla protezione dei dati, per quanto riguarda l'applicazione della legge relativa alla lotta all'attività informatica malevola;

61. invita tutti gli Stati membri a incentrare le strategie nazionali in materia di sicurezza informatica sulla protezione dei sistemi di informazione e dei dati associati e a considerare la protezione delle infrastrutture critiche come una parte del loro rispettivo dovere di diligenza; esorta gli Stati membri ad adottare e attuare strategie, linee guida e strumenti che forniscano livelli di protezione ragionevoli contro livelli di minaccia ragionevolmente identificabili, in cui i costi e gli oneri della protezione siano commisurati al possibile danno che le parti interessate rischiano di subire; invita gli Stati membri ad adottare misure appropriate per obbligare le persone giuridiche nella loro giurisdizione a proteggere i dati personali loro affidati;

62. riconosce che, a causa dell'evoluzione del contesto delle minacce informatiche, potrebbe essere consigliabile una cooperazione più intensa e strutturata con le forze di polizia, in particolare in alcuni ambiti critici, ad esempio nel localizzare le minacce connesse alla jihad informatica, il terrorismo informatico, la radicalizzazione online e il finanziamento di organizzazioni estremiste o radicali;

63. incoraggia una stretta cooperazione tra le agenzie dell'UE, come l'AED, l'ENISA e il Centro europeo per la lotta alla criminalità informatica, in un approccio transettoriale mirato a promuovere sinergie ed evitare sovrapposizioni;

64. invita la Commissione a elaborare una tabella di marcia per un approccio coordinato alla ciberdifesa europea, tra cui un aggiornamento del quadro strategico dell'UE in materia di ciberdifesa al fine di garantire che lo strumento continui a essere utile in qualità di meccanismo strategico pertinente per conseguire gli obiettivi dell'UE in materia di ciberdifesa, in stretta cooperazione con gli Stati membri, l'AED, il Parlamento e il SEAE; osserva che tale processo deve rientrare in un approccio strategico più ampio alla PSDC;

65. chiede la creazione di capacità di cibersicurezza attraverso la cooperazione allo sviluppo, nonché l'istruzione e la formazione continue in materia di sensibilizzazione informatica, tenendo conto del fatto che nei prossimi anni vi saranno milioni di nuovi utenti di Internet, la maggior parte dei quali nei paesi in via di sviluppo, rafforzando così la resilienza dei paesi e delle società rispetto alle minacce informatiche e ibride;

66. chiede una cooperazione internazionale e iniziative multilaterali per creare quadri rigorosi di ciberdifesa e cibersicurezza per combattere il rischio di Stati ostaggio della corruzione, della frode finanziaria, del riciclaggio di denaro e del finanziamento del terrorismo, nonché per affrontare le sfide poste dal ciberterrorismo, dalle criptovalute e da altri metodi di pagamento alternativi;

67. osserva che i ciberattacchi come NotPetya si diffondono rapidamente, causando in tal modo danni indiscriminati, a meno che non vi sia una resilienza diffusa a livello globale; ritiene che la formazione e l'istruzione in materia di ciberdifesa debbano far parte dell'azione esterna dell'UE e che la creazione della resilienza informatica nei paesi terzi contribuisca alla pace e alla sicurezza internazionali rendendo in ultima analisi i cittadini europei più sicuri;

Rafforzamento istituzionale

68. invita gli Stati membri a impegnarsi in una cooperazione più ambiziosa nel settore informatico nell'ambito della CSP; propone che gli Stati membri avviino un nuovo programma di cooperazione strutturata permanente (PESCO) in ambito informatico per sostenere una pianificazione, un comando e un controllo rapidi ed efficaci delle operazioni e delle missioni attuali e future dell'UE; osserva che ciò dovrebbe comportare un miglior coordinamento delle capacità operative nel ciberspazio e può condurre allo sviluppo di un comando di ciberdifesa comune qualora il Consiglio europeo decida in tal senso;

69. ribadisce il suo invito agli Stati membri e al VP/AR a presentare un Libro bianco dell'UE in materia di sicurezza e difesa; invita gli Stati membri e il VP/AR a rendere la ciberdifesa e la deterrenza informatica una pietra miliare del Libro bianco che tratti sia la protezione del settore informatico per le operazioni di cui all'articolo 43 TUE che la difesa comune di cui all'articolo 42, paragrafo 7, TUE;

70. osserva che il nuovo programma di cooperazione informatica PESCO dovrebbe essere condotto da personale militare e civile di grado elevato proveniente da ciascuno Stato membro, a rotazione, e rispondere ai ministri della Difesa dell'UE, nel formato PESCO, e al VP/AR, al fine di promuovere i principi della fiducia tra gli Stati membri e le istituzioni e agenzie dell'UE in sede di scambio di informazioni e dati;

71. ribadisce la sua richiesta di creare un Consiglio dell'Unione europea sulla difesa sulla base del comitato direttivo ministeriale dell'AED esistente e del formato PESCO dei ministri della Difesa dell'UE, al fine di garantire l'attribuzione di priorità, l'operatività delle risorse e cooperazione e integrazione efficaci tra gli Stati membri;

72. ricorda la necessità di garantire che il Fondo europeo per la difesa sia mantenuto o persino rafforzato nel prossimo QFP, con un bilancio sufficiente destinato alla ciberdifesa informatica;

73. chiede di aumentare le risorse per modernizzare e razionalizzare la cibersicurezza e la diffusione delle informazioni tra il SEAE/Centro dell'UE di analisi dell'intelligence (INTCEN), il Consiglio e la Commissione;

Partenariati pubblico-privato

74. riconosce che le imprese private svolgono un ruolo fondamentale nel prevenire, individuare e contenere gli incidenti di cibersicurezza, non solo come fornitori industriali di tecnologia ma anche come fornitori di servizi non informatici;

75. riconosce il ruolo del settore privato nella prevenzione, nell'individuazione e nel contenimento degli incidenti di cibersicurezza nonché nella risposta agli stessi, unitamente al suo ruolo nella promozione dell'innovazione nell'ambito della ciberdifesa, e chiede pertanto di rafforzare la cooperazione con il settore privato per garantire una comprensione comune dei requisiti dell'UE e della NATO e assistenza nel contribuire a trovare soluzioni comuni;

76. invita l'UE a effettuare una revisione globale delle apparecchiature e delle infrastrutture di software, informatiche e di comunicazione utilizzate nelle istituzioni al fine di escludere programmi e dispositivi potenzialmente pericolosi e vietare quelli confermati come malevoli, per esempio Kaspersky Lab;

o

o o

77. incarica il suo Presidente di trasmettere la presente risoluzione al Consiglio europeo, al Consiglio, alla Commissione, al vicepresidente della Commissione / alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, alle agenzie dell'UE nei campi della difesa e della cibersicurezza, al Segretario generale della NATO e ai parlamenti nazionali degli Stati membri dell'UE.