Consiglio
dell'Unione europea

**Bruxelles, 20 novembre 2017**
**(OR. en)**

**14435/17**

**CYBER 183**
**TELECOM 303**
**ENFOPOL 534**
**JAI 1055**
**MI 845**
**COSI 283**
**JAIEX 101**
**RELEX 989**
**IND 317**
**CSDP/PSDC 643**
**COPS 360**
**POLMIL 145**

**RISULTATI DEI LAVORI**

| | |
|---|---|
| Origine: | Segretariato generale del Consiglio |
| in data: | 20 novembre 2017 |
| Destinatario: | delegazioni |
| n. doc. prec.: | 13943/17 + COR 1 |
| n. doc. Comm.: | 12210/17, 12211/17 |
| Oggetto: | Conclusioni del Consiglio sulla comunicazione congiunta al Parlamento europeo e al Consiglio: Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE<br>- Conclusioni del Consiglio (20 novembre 2017) |

Si allegano per le delegazioni le conclusioni del Consiglio sulla comunicazione congiunta al Parlamento europeo e al Consiglio: Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE, adottate dal Consiglio "Affari generali" del 20 novembre 2017.

**ALLEGATO**

**Progetto di conclusioni del Consiglio sulla comunicazione congiunta al Parlamento europeo e al Consiglio "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE**

Il Consiglio dell'Unione europea,

1. RICONOSCENDO l'importanza della cibersicurezza per la prosperità, la crescita e la sicurezza dell'UE nonché per l'integrità delle nostre società libere e democratiche e dei processi che li sostengono nell'era digitale, dal momento che essa tutela sia lo stato di diritto che i diritti umani e le libertà fondamentali di ciascun individuo;

2. SOTTOLINEANDO la necessità di affrontare la cibersicurezza con un approccio coerente a livello nazionale, dell'UE e mondiale, dal momento che le minacce informatiche possono avere un impatto sulla nostra democrazia, prosperità, stabilità e sicurezza;

3. OSSERVA che un livello elevato di ciberresilienza in tutta l'UE è altresì importante per conseguire la fiducia nel mercato unico digitale e l'ulteriore sviluppo di un'Europa digitale;

4. RIBADENDO che l'UE promuoverà costantemente un ciberspazio aperto, globale, libero, pacifico e sicuro, in cui siano pienamente applicati e rispettati i diritti umani e le libertà fondamentali, in particolare il diritto alla libertà di espressione, l'accesso all'informazione, la protezione dei dati, la tutela della vita privata e della sicurezza, nonché i valori e i principi fondamentali dell'UE, sia all'interno della stessa che a livello mondiale, e METTENDO IN RILIEVO l'importanza cruciale di garantire un adeguato equilibrio tra i diritti umani e le libertà fondamentali, da un lato, e il rispetto dei requisiti della politica di sicurezza interna dell'UE, dall'altro[1],

5. RICONOSCENDO che il diritto internazionale, compresa la Carta delle Nazioni Unite in tutti i suoi elementi, il diritto internazionale umanitario e il diritto in materia di diritti umani sono di applicazione nel ciberspazio e SOTTOLINEANDO pertanto la necessità di proseguire gli sforzi volti a garantire che in tale ambito venga rispettato il diritto internazionale;

[1] Doc. 12650/17.

6. RAMMENTANDO le sue conclusioni sulla strategia dell'Unione europea per la cibersicurezza[2], sulla governance di internet[3], sul rafforzamento del sistema di resilienza informatica dell'Europa[4] sulla diplomazia informatica[5] e su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose[6], sul miglioramento della giustizia penale nel ciberspazio[7], sulla sicurezza e la difesa nel contesto della strategia globale dell'UE[8], su un quadro congiunto per contrastare le minacce ibride[9] e sulla revisione intermedia della rinnovata strategia di sicurezza interna dell'Unione europea 2015-2020[10];

7. RICONOSCENDO che il quadro previsto dalla convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica (la convenzione di Budapest) offre a un gruppo eterogeneo di paesi una base solida per l'utilizzo di uno standard giuridico efficace per le diverse legislazioni nazionali e per la cooperazione internazionale in materia di cibercriminalità;

8. RICONOSCENDO la necessità di dare nuova enfasi all'attuazione del quadro strategico dell'UE in materia di ciberdifesa del 2014 e di aggiornare tale quadro per integrare ulteriormente la cibersicurezza e la difesa nella politica di sicurezza e di difesa comune (PSDC) e nella più ampia agenda in materia di sicurezza e difesa;

9. RICONOSCENDO che un'industria europea competitiva a livello mondiale è un elemento importante per raggiungere un elevato livello di cibersicurezza a livello nazionale e dell'UE;

10. RICORDANDO che, a norma dell'articolo 4, paragrafo 2, del TUE, la sicurezza nazionale è di esclusiva competenza di ciascuno Stato membro.

---

2 Doc. 12109/13 e doc. 6225/13 (Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni: Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro (COM JOIN (2013) 1 final).

3 Doc. 16200/14 e doc. 6460/14 (Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - Governance e politica di internet – Il ruolo dell'Europa nel forgiare il futuro della governance di internet (COM(2014) 72 final).

4 Doc. 14540/16 e doc. 11013/16 (Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza (COM 2016(410) final).

5 Doc. 6122/15.

6 Doc. 9916/17.

7 Doc. 10007/16.

8 Doc. 9178/17.

9 Doc. 7688/16 (Comunicazione congiunta al Parlamento europeo e al Consiglio - Quadro congiunto per contrastare le minacce ibride: La risposta dell'Unione europea).

10 Doc. 12650/17.

**CON LE PRESENTI CONCLUSIONI**

11. ACCOGLIE CON FAVORE la comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE", che propone l'ambizioso obiettivo di rafforzare la cibersicurezza all'interno dell'UE. Essa contribuisce inoltre all'autonomia strategica dell'UE, come indicato nelle conclusioni sulla strategia globale per la politica estera e di sicurezza dell'Unione europea[11], prefiggendosi di costruire un'Europa digitale che sia più sicura, ispiri fiducia, sia consapevole dei propri punti di forza, competitiva, aperta al mondo, rispettosa dei valori condivisi dell'UE per quanto riguarda un internet globale aperto, libero, pacifico e sicuro e, di conseguenza, di conseguire un più elevato livello di resilienza onde prevenire, dissuadere, individuare le minacce informatiche e di reagirvi, nonché essere in grado di dare una risposta comune alle minacce cibernetiche in tutta l'UE, e

12. INVITA gli Stati membri nonché le istituzioni, le agenzie e gli organismi dell'UE a collaborare, nel rispetto delle rispettive aree di competenza e del principio di sussidiarietà e proporzionalità, per rispondere agli obiettivi strategici stabiliti nelle presenti conclusioni, e

13. SOTTOLINEA la necessità che l'UE, i suoi Stati membri e il settore privato assicurino finanziamenti adeguati nel rispetto delle risorse disponibili per sostenere il potenziamento degli sforzi di ricerca e sviluppo in materia di cibersicurezza e ciberresilienza in tutta l'Unione europea, nonché per rafforzare la cooperazione al fine di prevenire, dissuadere, individuare le minacce informatiche e per reagirvi ed essere in grado di dare una risposta comune ai ciberincidenti e alle attività informatiche dolose su vasta scala;

---

[11] Doc. 13202/16.

**Capo I**

**GARANTIRE UN'EFFICACE CIBERRESILIENZA DELL'UE E LA FIDUCIA NEL MERCATO UNICO DIGITALE**

14. SOTTOLINEA che ciascuno Stato membro ha la responsabilità primaria di rafforzare la propria cibersicurezza e di garantire la propria risposta agli incidenti e alle crisi di cibersicurezza, mentre l'UE può apportare un forte valore aggiunto sostenendo la cooperazione tra gli Stati membri. In tale contesto EVIDENZIA la necessità che tutti gli Stati membri mettano a disposizione delle autorità nazionali responsabili della cibersicurezza le risorse necessarie al fine di garantire la prevenzione, l'individuazione e la risposta agli incidenti e alle crisi di cibersicurezza in tutta l'UE;

15. SOTTOLINEA la necessità, ove possibile, di avvalersi dei meccanismi, delle strutture e degli organismi esistenti a livello dell'UE;

16. ELOGIA:

- i progressi compiuti nel recepimento della direttiva NIS da parte degli Stati membri e SOTTOLINEA la necessità di conseguire una piena ed efficace attuazione entro maggio 2018, come previsto nella direttiva stessa[12];
- il lavoro svolto nell'ambito del gruppo di cooperazione NIS al fine di migliorare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri;
- il lavoro svolto nell'ambito della rete di CSIRT, in particolare per rafforzare la cooperazione operativa fra gli Stati membri, creare un clima di fiducia nello scambio di informazioni per la gestione degli incidenti in materia di cibersicurezza su vasta scala e, sulla base delle conclusioni nazionali degli Stati membri, per fornire elementi per una conoscenza situazionale condivisa a livello europeo;
- il lavoro svolto nell'ambito del partenariato pubblico-privato sulla cibersicurezza.

[12] Fatta salva la competenza degli Stati membri per il recepimento della direttiva NIS, in particolare per quanto riguarda gli operatori di servizi essenziali.

17. SI COMPIACE che la comunicazione congiunta confermi che una cifratura forte e affidabile riveste un'importanza cruciale per un'adeguata garanzia dei diritti umani e delle libertà fondamentali nell'UE nonché per la fiducia del pubblico nel mercato unico digitale, pur tenendo conto della necessità delle autorità di contrasto di accedere ai dati necessari per le loro indagini, e che essa confermi altresì che l'identificazione e la comunicazione digitali sicure rivestono un ruolo essenziale per garantire una cibersicurezza efficace nell'UE;

18. ACCOGLIE CON FAVORE l'intenzione espressa nella comunicazione congiunta di accrescere il livello di ambizione realizzando esercitazioni di cibersicurezza paneuropee a intervalli regolari, sulla base delle esperienze maturate con le esercitazioni Cyber Europe, che combinino la risposta a diversi livelli, in quanto sarà importante per rafforzare la preparazione degli Stati membri e delle istituzioni dell'UE nella risposta ai ciberincidenti su vasta scala;

19. INVITA l'UE e i suoi Stati membri a condurre periodicamente esercitazioni di cibersicurezza strategici in varie formazioni del Consiglio, basandosi sull'esperienza acquisita nel corso di EU CYBRID 2017 e

20. Fatto salvo il risultato del processo legislativo:

- ACCOGLIE CON FAVORE la proposta di un mandato forte e permanente per l'ENISA con l'obiettivo primario di sostenere e sviluppare una più stretta cooperazione tra gli Stati membri, incrementare le loro capacità e accrescere la fiducia in un'Europa digitale;

- RIBADISCE che la futura ENISA dovrebbe avvalersi dell'esperienza e delle competenze all'interno degli Stati membri e dell'UE e sostenere lo sviluppo e l'attuazione coerenti delle attuali e future politiche e norme di cibersicurezza dell'UE, assicurando al contempo che tutte le sue competenze siano sviluppate a complemento di quelle degli Stati membri;

- RIBADISCE l'obiettivo di accrescere la fiducia in un'Europa digitale aumentando l'affidamento sulle soluzioni e innovazioni digitali, tra cui l'Internet delle cose, il commercio elettronico e la governance elettronica, in particolare attraverso un quadro europeo di certificazione della cibersicurezza di rilevanza mondiale[13]. Si tratta di un requisito fondamentale per migliorare la fiducia e la sicurezza nei prodotti e nei servizi digitali nonché per proteggere le infrastrutture critiche e i dati governativi, dei cittadini e delle imprese ed è di fondamentale importanza per l'adozione di un approccio basato sul concetto della sicurezza sin dalla progettazione per i prodotti, i servizi e i processi nel mercato unico digitale;

- SOTTOLINEA che l'attività legislativa intesa a rafforzare la certificazione della cibersicurezza a livello dell'UE dovrà rispondere alle esigenze del mercato e degli utenti, basarsi sulle esperienze relative ai processi e alle capacità di certificazione esistenti nell'UE (ad esempio il quadro SOG-IS) e dovrebbe fornire un quadro in grado di adattarsi rapidamente ai futuri sviluppi digitali d'avanguardia;

- SOTTOLINEA che il rafforzamento della certificazione della cibersicurezza nell'UE dovrebbe contemplare l'intera gamma dei requisiti di sicurezza, compresi quelli più rigorosi, in cui va dimostrata la resistenza alle capacità degli autori degli attacchi. Tra i principali fattori di successo figurano: garantire un processo affidabile, trasparente e indipendente per la certificazione della sicurezza al fine di promuovere la disponibilità di dispositivi, software e servizi affidabili e sicuri all'interno del mercato unico e oltre; riconoscere le rispettive competenze dell'industria europea, dei governi e degli specialisti della valutazione mediante norme europee e mondiali[14]; rispettare il ruolo degli Stati membri nel processo di certificazione, in particolare per quanto concerne la valutazione a livelli di sicurezza più elevati e in particolare in relazione alle esigenze essenziali di sicurezza e alla valutazione delle competenze. Tale quadro di certificazione dovrebbe inoltre garantire che qualsiasi sistema di certificazione a livello dell'Unione sia proporzionato al livello di garanzia necessario per l'utilizzo dei prodotti, dei servizi e/o dei sistemi TIC interessati e consenta scambi transfrontalieri per le imprese di tutte le dimensioni affinché sviluppino e vendano nuovi prodotti, sia all'interno dell'UE che al di fuori dei suoi mercati.

---

**13** Attraverso norme globali sviluppate conformemente allo spirito dell'OMC - Codice di buone prassi sugli ostacoli tecnici agli scambi.

**14** Attraverso norme europee e globali sviluppate conformemente allo spirito dell'OMC - Codice di buone prassi sugli ostacoli tecnici agli scambi.

21. ACCOGLIE CON FAVORE l'intenzione di istituire una rete di centri di competenza sulla cibersicurezza per stimolare lo sviluppo e l'impiego di tecnologie di cibersicurezza e dare uno stimolo aggiuntivo all'innovazione dell'industria dell'UE sulla scena globale nello sviluppo di tecnologie di prossima generazione e innovative, tra cui intelligenza artificiale, informatica quantistica, blockchain e identità digitali sicure;

22. SOTTOLINEA la necessità che la rete di centri di competenza sulla cibersicurezza sia inclusiva nei confronti di tutti gli Stati membri e dei loro centri di eccellenza e competenza esistenti e presti particolare attenzione alla complementarietà e, tenendo a mente questo aspetto, PRENDE ATTO del previsto centro europeo di ricerca sulla cibersicurezza, il cui ruolo chiave dovrebbe essere quello di garantire la complementarità e evitare duplicazioni all'interno della rete di centri di competenza sulla cibersicurezza e con altre agenzie dell'UE;

23. SOTTOLINEA che la rete di centri di competenza sulla cibersicurezza dovrebbe trattare una gamma di questioni che vanno dalla ricerca all'industria e dovrebbe pertanto contribuire tra l'altro al conseguimento dell'obiettivo dell'autonomia strategica dell'Europa;

24. In relazione alla rete di centri di competenza sulla cibersicurezza proposta, RIBADISCE la necessità che l'UE, attraverso i suoi Stati membri, sviluppi una capacità europea per valutare la forza della crittografia utilizzata in prodotti e servizi disponibili per i cittadini, le imprese e i governi all'interno del mercato unico digitale, pur riconoscendo che le politiche in materia di crittografia sono un aspetto chiave della sicurezza nazionale e rientrano pertanto nell'ambito di competenza degli Stati membri;

25. INVITA tutte le parti interessate ad aumentare gli investimenti nelle applicazioni di cibersicurezza delle nuove tecnologie al fine di contribuire a garantire la cibersicurezza in tutti i settori dell'economia europea;

26. Sottolinea l'importanza, per le istituzioni dell'UE, di fornire servizi in materia di cibersicurezza credibili, affidabili e coordinati e INVITA la COMISSIONE e le altre istituzioni dell'UE a sviluppare ulteriormente la CERT-UE in base a tali obiettivi e a garantire inoltre risorse adeguate a tal fine;

27. ACCOGLIE CON FAVORE l'invito a riconoscere l'importante ruolo dei ricercatori terzi in materia di sicurezza ai fini della scoperta di vulnerabilità nei prodotti e servizi esistenti e INVITA gli Stati membri a condividere le migliori prassi per la divulgazione coordinata delle vulnerabilità;

28. SOTTOLINEA la responsabilità di ognuno in materia di cibersicurezza e INVITA l'UE e gli Stati membri a promuovere le competenze digitali e l'alfabetizzazione mediatica per aiutare gli utenti a proteggere le loro informazioni digitali online e sensibilizzarli sui rischi dell'inserimento di dati personali in internet;

29. ACCOGLIE CON FAVORE l'enfasi posta dalla comunicazione congiunta sull'istruzione, nonché sull'igiene e la consapevolezza cibernetiche negli Stati membri e nell'UE;

30. INVITA LA COMMISSIONE a fornire rapidamente una valutazione d'impatto e a proporre entro la metà del 2018 gli strumenti giuridici pertinenti per l'attuazione dell'iniziativa che istituisce una rete di centri di competenza sulla cibersicurezza e un centro europeo di ricerca e di competenza sulla cibersicurezza;

31. INVITA gli Stati membri a:

- dare la priorità alla consapevolezza cibernetica nelle campagne di informazione e promuovere la cibersicurezza nei programmi di formazione accademica, scolastica e professionale. Particolare attenzione deve essere rivolta alla promozione dell'istruzione per i giovani e delle competenze digitali, per creare professionisti in grado di affrontare le sfide future nei settori della sicurezza, dell'economia e dei servizi;

- proseguire gli sforzi volti all'avvio di programmi specializzati ad alto livello in materia di cibersicurezza al fine di rimediare all'attuale penuria di operatori della cibersicurezza nell'UE;

- creare una rete di cooperazione efficace tra punti di contatto nel settore dell'istruzione sotto l'egida dell'ENISA. La rete di punti di contatto dovrebbe mirare a rafforzare il coordinamento e lo scambio di migliori pratiche tra gli Stati membri nel settore dell'istruzione e della sensibilizzazione in materia di cibersicurezza, nonché di formazione, esercitazioni e sviluppo di capacità;

- prendere in considerazione l'applicazione della direttiva NIS anche alle pubbliche amministrazioni che partecipano ad attività sociali o economiche fondamentali, se non sono già contemplate dalla legislazione nazionale e se lo ritiene opportuno, nonché fornire una formazione in materia di cibersicurezza anche presso le amministrazioni pubbliche, dato il ruolo da esse svolto nell'ambito della nostra società ed economia.

**Capo II**

**COSTRUIRE LA CAPACITÀ DELL'UE DI PREVENIRE, DISSUADERE, INDIVIDUARE E AFFRONTARE LE ATTIVITÀ INFORMATICHE DOLOSE**

32. SOTTOLINEA che un incidente o una crisi cibernetica particolarmente grave potrebbe costituire una motivazione sufficiente perché uno Stato membro invochi la clausola di solidarietà[15] e/o la clausola di assistenza reciproca[16] dell'UE.

33. ACCOGLIE CON FAVORE l'adozione del "quadro per una risposta diplomatica congiunta dell'UE alle attività informatiche dolose", che contribuisce alla prevenzione dei conflitti, alla cooperazione e alla stabilità nel ciberspazio stabilendo misure in ambito PESC, comprese misure restrittive, che possono essere utilizzate per prevenire e affrontare le attività informatiche dolose e INVITA il SEAE e gli Stati membri a realizzare esercitazioni periodiche in tale quadro;

---

15 Articolo 222 del TFUE
16 Articolo 42, paragrafo 7 del TUE

34. SOTTOLINEA la necessità di rispondere in modo efficace agli incidenti e alle crisi di cibersicurezza su vasta scala a livello UE, nel rispetto delle competenze degli Stati membri, nonché l'esigenza di integrare la cibersicurezza nei meccanismi esistenti di gestione delle crisi a livello UE[17]. Al fine di conseguire tale obiettivo, CHIEDE che a livello UE siano organizzate regolarmente esercitazioni per verificare la risposta a seguito di incidenti di cibersicurezza su vasta scala - sul piano sia diplomatico-strategico sia tecnico - sulla base dei quadri e delle procedure pertinenti, anche perfezionandole, se del caso[18];

35. SOTTOLINEA l'importanza di una risposta ben integrata e di meccanismi per lo scambio di informazioni tra le diverse comunità, elementi fondamentali per garantire la cibersicurezza in Europa, anche tra gli organi competenti dell'UE e le autorità degli Stati membri. Tali meccanismi dovranno essere testati e verificati nell'ambito di esercitazioni di cibersicurezza a livello UE e formalizzati da rispettivi accordi, se necessario;

36. PRENDE ATTO della possibilità di esaminare, qualora la Commissione dovesse presentare una proposta relativa all'istituzione di un Fondo di risposta alle emergenze di cibersicurezza in aggiunta agli attuali sforzi degli Stati membri e rispettando le risorse disponibili (in particolare nell'ambito del quadro finanziario pluriennale dell'UE), l'ipotesi di assistere gli Stati membri nella risposta e mitigazione degli incidenti di cibersicurezza su vasta scala, purché lo Stato membro si sia dotato, prima dell'incidente, di un sistema prudente di cibersicurezza che comprenda la piena attuazione della direttiva NIS, una gestione matura dei rischi e quadri di vigilanza a livello nazionale.

37. RICONOSCE i crescenti legami tra cibersicurezza e difesa e CHIEDE di rafforzare la cooperazione in materia di ciberdifesa, anche promuovendo la cooperazione tra le comunità incaricate della risposta agli incidenti civili e militari, nonché di continuare a rafforzare la cibersicurezza delle missioni e delle operazioni PSDC;

---

**17** C(2017) 6100 final
**18** 9916/17 e C(2017) 6100 final

38. SOTTOLINEA la necessità, se del caso, di utilizzare appieno le proposte di iniziative nel settore della difesa per accelerare lo sviluppo di adeguate capacità cibernetiche in Europa e RICONOSCE le opportunità insite nell'eventuale elaborazione di progetti in materia di ciberdifesa attraverso la PESCO, se gli Stati membri che vi partecipano lo ritengono necessario; RICONOSCE inoltre il ruolo svolto dalla base industriale e tecnologica di difesa europea (EDTIB) e dalla più ampia base industriale della cibersicurezza civile nel fornire agli Stati membri gli strumenti per tutelare i loro interessi in materia di cibersicurezza e ciberdifesa;

39. PRENDE ATTO della proposta della Commissione volta a istituire una piattaforma di istruzione e di formazione in materia di ciberdifesa entro la fine del 2018 e SOTTOLINEA che la piattaforma dovrebbe aumentare le possibilità di formazione e di istruzione all'interno degli Stati membri e garantire la complementarità con altri sforzi e iniziative dell'UE, in particolare con l'AESD e l'AED;

40. INVITA l'UE e gli Stati membri a rispondere alla minaccia di furti di proprietà intellettuale basati sulle TIC, compresi i segreti commerciali o altre informazioni commerciali riservate, intesi a fornire vantaggi competitivi a società o settori commerciali;

41. RICONOSCE la necessità di affrontare reati nel ciberspazio, compresi quelli compiuti nel "dark web", lo sfruttamento sessuale di minori online, nonché la frode e la falsificazione degli strumenti di pagamento diversi dai contanti, in particolare al fine di migliorare il quadro di intelligence, svolgendo indagini congiunte e condividendo il supporto operativo;

42. ACCOGLIE CON FAVORE il lavoro svolto dall'UE e dagli Stati membri nell'affrontare le sfide poste da sistemi che consentono a criminali e terroristi di comunicare in modi inaccessibili alle autorità competenti, SOTTOLINEA che questo lavoro deve tener conto del fatto che una cifratura forte e affidabile riveste un'importanza cruciale per la cibersicurezza e per la fiducia nel mercato unico digitale e per garantire il rispetto dei diritti umani e delle libertà fondamentali;

43. SOTTOLINEA l'importanza di fornire alle autorità di contrasto strumenti che consentano di individuare, investigare e perseguire la cibercriminalità, affinché i reati commessi nel ciberspazio non passino inosservati o restino impuniti e ACCOGLIE CON FAVORE il contributo della rete giudiziaria europea per la criminalità informatica nell'ambito della lotta contro la criminalità attraverso la cooperazione tra le autorità giudiziarie;

44. SOTTOLINEA l'importanza di assicurare una posizione coordinata dell'UE per predisporre in modo efficace le decisioni sulla governance di internet a livello europeo e mondiale nell'ambito della comunità multipartecipativa, ad esempio garantendo che le banche dati WHOIS degli indirizzi IP e dei nomi di dominio siano accurate e di facile accesso, in modo da salvaguardare le capacità di contrasto e gli interessi pubblici;

45. SOTTOLINEA l'importanza di diffondere il protocollo internet IPv6, che è di vitale importanza per lo sviluppo dell'"internet delle cose" su vasta scala, nonché per migliorare l'attribuzione dei reati nel ciberspazio;

46. INCORAGGIA i lavori in corso in materia di accesso transfrontaliero alle prove elettroniche, di conservazione dei dati e per far fronte alle difficoltà che pongono per i procedimenti penali i sistemi che consentono a criminali e terroristi di comunicare in modi inaccessibili alle autorità competenti, tenendo conto della necessità di rispettare i diritti umani e le libertà fondamentali, nonché la protezione dei dati;

47. INVITA la Commissione a:

- presentare entro dicembre 2017 una relazione sui progressi compiuti nell'attuazione delle misure pratiche per migliorare l'accesso transfrontaliero alle prove elettroniche;
- presentare all'inizio del 2018 una proposta legislativa volta a migliorare l'accesso transfrontaliero alle prove elettroniche;

48. INVITA l'Europol, l'ENISA ed Eurojust a:

- continuare a rafforzare la loro cooperazione nella lotta contro la cibercriminalità, sia tra di loro sia con altre parti interessate, compresi la comunità della CSIRT, l'Interpol, il settore privato e il mondo accademico, garantendo le sinergie e le complementarità, conformemente ai rispettivi mandati e competenze;

- contribuire, in collaborazione con gli Stati membri, a un approccio coordinato ai fini della risposta da parte delle autorità di contrasto dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala, volto ad integrare le procedure definite nei quadri pertinenti[19];

49. INVITA l'UE e gli Stati membri a proseguire i lavori volti a:

- eliminare gli ostacoli alle indagini in materia di criminalità e all'efficacia della giustizia penale nel ciberspazio, nonché a rafforzare la cooperazione e il coordinamento a livello internazionale nella lotta contro la criminalità nel ciberspazio;

- affrontare le sfide poste dalle tecnologie di anonimizzazione, tenendo presente che una cifratura forte e affidabile riveste grande importanza per la cibersicurezza e per la fiducia nel mercato unico digitale;

- predisporre decisioni sulla governance di internet che abbiano un impatto sulle capacità di contrasto nella lotta contro la criminalità nel ciberspazio;

[19] 9916/17 e C(2017) 6100 final.

**Capo III**

**RAFFORZARE LA COOPERAZIONE INTERNAZIONALE PER UN CIBERSPAZIO APERTO, LIBERO PACIFICO E SICURO A LIVELLO MONDIALE**

50. RICONOSCE che garantire la cibersicurezza è una sfida mondiale che richiede una cooperazione efficace sul piano globale tra tutti i soggetti e RICONOSCE che occorre riservare particolare attenzione al rispetto dei valori democratici e dei principi di un ciberspazio aperto, libero, pacifico e sicuro a livello mondiale; in tale prospettiva,

51. INVITA l'UE e gli Stati membri a promuovere l'istituzione di un quadro strategico per la prevenzione dei conflitti, la cooperazione e la stabilità nel ciberspazio, fondato sull'applicazione del diritto internazionale vigente, e in particolare della Carta delle Nazioni Unite nella sua interezza, sullo sviluppo e l'attuazione di norme universali per un comportamento responsabile da parte degli Stati, nonché su misure regionali di rafforzamento della fiducia tra gli Stati;

52. RICONOSCE il ruolo delle Nazioni Unite nell'ulteriore sviluppo di norme per un comportamento responsabile da parte degli Stati nel ciberspazio e ricorda che i risultati delle discussioni in sede di gruppo di esperti governativi delle Nazioni Unite nel corso degli anni hanno formulato una serie consensuale di norme e raccomandazioni[20], che l'Assemblea generale ha ripetutamente avallato, e che gli Stati membri dovrebbero adottare come base per il loro comportamento responsabile nel ciberspazio;

53. RICONOSCE che, nell'ambito di tali norme di comportamento responsabile, gli Stati non dovrebbero consentire consapevolmente l'utilizzo dei rispettivi territori per atti illeciti a livello internazionale, che dovrebbero rispondere a richieste di assistenza appropriate da parte di un altro Stato la cui infrastruttura critica è oggetto di atti dolosi nell'ambito delle TIC commessi sul loro territorio, e che dovrebbero adottare le misure necessarie per proteggere le loro infrastrutture critiche dalle minacce alle TIC;

54. RICONOSCE il carattere condiviso delle minacce e dei rischi in materia di cibersicurezza cui devono far fronte l'UE, la NATO e i rispettivi Stati membri e RIBADISCE l'importanza di proseguire la cooperazione tra l'UE e la NATO in materia di cibersicurezza e difesa nel pieno rispetto dei principi di inclusione, reciprocità e autonomia decisionale dell'UE e in linea con le sue conclusioni del 6 dicembre 2016 sull'attuazione della dichiarazione congiunta del presidente del Consiglio europeo, del presidente della Commissione europea e del Segretario generale dell'Organizzazione del Trattato del Nord Atlantico[20];

55. INVITA l'UE e gli Stati membri a sostenere e incoraggiare lo sviluppo di misure volte a rafforzare la fiducia a livello regionale, che costituiscono un elemento essenziale per rafforzare la collaborazione e la trasparenza e ridurre il rischio di conflitto. L'attuazione di misure di rafforzamento della fiducia nella cibersicurezza in ambito OSCE e in altri contesti regionali aumenterà la prevedibilità del comportamento degli Stati e contribuirà ulteriormente a stabilizzare il ciberspazio;

56. RIBADISCE che l'UE continuerà a difendere i suoi valori fondamentali in materia di tutela dei diritti umani e delle libertà fondamentali sulla base degli orientamenti dell'UE in materia di diritti umani sulla libertà online. L'UE sottolinea inoltre l'importanza che riveste il coinvolgimento di tutte le parti interessate nella governance di internet, compreso il mondo accademico, la società civile e il settore privato;

57. INVITA l'UE e gli Stati membri a promuovere la creazione di capacità cibernetiche nei paesi terzi, dando una priorità speciale ai vicini dell'UE che si trovano in una fase di rapida crescita della connettività, per far fronte alla cibercriminalità, nonché a sviluppare la ciberresilienza, in conformità con i valori fondamentali dell'UE. Per far progredire gli sforzi dell'UE in questo settore, è opportuno porre in essere una rete dell'UE per lo sviluppo delle capacità cibernetiche, nonché orientamenti per lo sviluppo delle capacità cibernetiche, che dovrebbero essere complementari agli attuali meccanismi e strutture;

---

[20] Doc. 15283/16.

58. SOTTOLINEA i progressi compiuti nella cooperazione tra l'UE e la NATO in materia di ciberdifesa e cibersicurezza, nonché il suo sviluppo in materia di formazione, istruzione e concetti, evitando nel contempo inutili duplicazioni di sforzi laddove i requisiti si sovrappongono, e promuovendo l'interoperabilità attraverso norme e requisiti di ciberdifesa, e INVITA a proseguire la cooperazione in materia di esercitazioni di ciberdifesa (a livello di personale) e a condividere le migliori prassi per quanto riguarda la gestione delle crisi, evitando inutili duplicazioni di sforzi laddove i requisiti si sovrappongono, nel pieno rispetto della politica dell'UE in materia di esercitazioni e dei principi di inclusione, reciprocità e autonomia decisionale dell'UE;

59. RICONOSCE che la Convenzione del Consiglio d'Europa sulla criminalità informatica (convenzione di Budapest) offre un quadro giuridico efficace su cui fondare le normative nazionali in materia di cibercriminalità. INVITA tutti i paesi a elaborare quadri giuridici nazionali adeguati e a proseguire la cooperazione nell'ambito del quadro internazionale esistente offerto dalla convenzione di Budapest;

60. RAMMENTA i risultati dei dialoghi bilaterali dell'UE in materia di cibersicurezza e invita a compiere ulteriori sforzi per agevolare la cooperazione con i paesi terzi in materia di cibersicurezza;

61. RICORDA che l'Unione europea dispone di un solido meccanismo di controllo delle esportazioni, giuridicamente vincolante e basato sulle decisioni e le migliori pratiche elaborate nell'ambito dei regimi internazionali di non proliferazione e RILEVA le discussioni in corso in sede di Consiglio volte a migliorare ulteriormente il funzionamento di tali controlli; INVITA gli Stati membri a continuare ad affrontare, nel quadro dei pertinenti regimi internazionali di controllo delle esportazioni (ad es. l'intesa di Wassenaar), le applicazioni delle tecnologie innovative che risultano critiche per la cibersicurezza, al fine di assicurare un efficace controllo delle tecnologie critiche del futuro in tale materia.

62. Facendo seguito alle conclusioni del Consiglio europeo del 19 ottobre 2017[21], le presenti conclusioni saranno attuate tramite un piano d'azione che sarà adottato dal Consiglio prima della fine del 2017. Il piano d'azione costituisce un documento in evoluzione e sarà riesaminato e aggiornato periodicamente dal Consiglio.

---

[21] EUCO 14/17