Consiglio dell'Unione europea

Bruxelles, 10 dicembre 2019
(OR. en)

14972/19

HYBRID 56	**EDUC 478**
DISINFO 18	**AUDIO 118**
AG 68	**DIGIT 179**
PE 257	**INF 332**
DATAPROTECT 300	**COSI 252**
JAI 1307	**CSDP/PSDC 575**
CYBER 328	**COPS 360**
JAIEX 177	**POLMIL 129**
FREMP 176	**IPCR 23**
RELEX 1147	**PROCIV 100**
CULT 141	**CSC 294**

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
Destinatario:	delegazioni
Oggetto:	Sforzi complementari per rafforzare la resilienza e contrastare le minacce ibride - Conclusioni del Consiglio (10 dicembre 2019)

Si allegano per le delegazioni le conclusioni del Consiglio sugli sforzi complementari per rafforzare la resilienza e contrastare le minacce ibride, adottate nella 3739ª sessione del Consiglio del 10 dicembre 2019.

ALLEGATO

Conclusioni del Consiglio sugli sforzi complementari per rafforzare la resilienza e contrastare le minacce ibride

1. Il Consiglio rammenta le pertinenti conclusioni del Consiglio europeo[1] e del Consiglio[2] e riconferma il suo impegno a rafforzare la resilienza dell'Unione e degli Stati membri nei confronti di minacce ibride dalla natura multiforme e in continua evoluzione e a consolidare la cooperazione volta a individuarle, prevenirle e contrastarle.

2. Il Consiglio riconosce i progressi compiuti nell'attuazione del quadro congiunto per contrastare le minacce ibride (2016) e della comunicazione congiunta "Rafforzamento della resilienza e potenziamento delle capacità di affrontare minacce ibride" (2018), come pure del piano d'azione contro la disinformazione (2018) in linea con le pertinenti conclusioni del Consiglio.

3. La responsabilità principale di contrastare le minacce ibride ricade sugli Stati membri: gli sforzi a livello dell'UE sono di natura complementare e non pregiudicano la responsabilità esclusiva degli Stati membri nelle questioni di sicurezza nazionale. Per affrontare le minacce ibride serve un approccio globale alla sicurezza che coinvolga tutta l'amministrazione e l'intera società e sia esteso a tutti gli ambiti politici in maniera più strategica, coordinata e coerente. È importante che un approccio implicante tutta l'amministrazione sia seguito e messo in atto anche a livello dell'UE.

4. Nelle presenti conclusioni il Consiglio stabilisce le priorità per quanto riguarda la protezione delle nostre società, dei nostri cittadini e delle libertà, nonché della sicurezza della nostra Unione rispetto alle minacce ibride nel contesto dell'attuazione della nuova agenda strategica 2019-2024, promuovendo un approccio globale alla sicurezza tramite un miglior coordinamento, più risorse e capacità tecnologiche e partendo dal lavoro importante già realizzato in vari settori politici, anche nell'ambito della cooperazione dell'UE in materia di sicurezza e difesa.

---

1 In particolare le conclusioni del Consiglio europeo di giugno 2019, marzo 2019, dicembre 2018, ottobre 2018, giugno 2018, marzo 2018, giugno 2015 e marzo 2015.

2 In particolare, ST 10048/19, ST 6573/1/19 REV1, ST 10255/19, ST 12836/19, ST 7928/16.

5. Gli sforzi per proteggere le nostre istituzioni democratiche dalle minacce ibride devono in ogni caso rispettare i diritti fondamentali, tra i quali la tutela dei dati personali, la libertà di espressione e di informazione e la libertà di associazione, quali sanciti nella Carta dei diritti fondamentali.

6. L'UE e gli Stati membri dovrebbero continuare a predisporre, addestrare ed esercitare le capacità necessarie a individuare le attività ibride, analizzarne le fonti e rispondervi e sostenere il rafforzamento della resilienza a lungo termine degli Stati membri e delle istituzioni, degli organi e delle agenzie dell'UE di fronte alle minacce ibride, sfruttando appieno gli strumenti esistenti, destinati a tale scopo. Il Consiglio sottolinea la necessità di aggiornare il protocollo operativo dell'UE relativo al contrasto delle minacce ibride sulla scorta degli insegnamenti individuati e tratti dalle precedenti esercitazioni.

7. Il Consiglio sottolinea la persistente necessità di cooperare con le organizzazioni internazionali come l'ONU, l'OSCE e il Consiglio d'Europa e in consessi quali il G7 per difendere l'ordine globale basato su regole, anche per quanto riguarda il contrasto delle minacce ibride, tra l'altro grazie a misure di rafforzamento della fiducia e ad altre misure pertinenti.

8. Il Consiglio sottolinea l'impegno dell'UE a continuare la cooperazione, stretta e sinergica, con tutti i paesi partner coinvolti, anche fornendo loro supporto, in particolare con quelli del vicinato dell'UE, al fine di rafforzare la resilienza e contrastare le minacce ibride.

9. Il Consiglio chiede che si continuino a compiere sforzi duraturi per far avanzare la realizzazione di tutte le azioni connesse con il contrasto delle minacce ibride previste dall'insieme comune di proposte per l'attuazione delle dichiarazioni congiunte sulla cooperazione UE-NATO, anche nei settori della conoscenza situazionale, della comunicazione strategica, della prevenzione e della risposta alle crisi e del rafforzamento della resilienza. In questo contesto, ribadisce la necessità di consolidare ulteriormente il dialogo politico in tema di contrasto delle minacce ibride e di tenere periodiche esercitazioni parallele e coordinate (PACE), con la partecipazione di tutti gli Stati membri dell'UE e gli alleati NATO, e chiede una tempestiva messa a punto del nuovo piano PACE. Il Consiglio sottolinea la necessità di tenere conto degli insegnamenti individuati e dell'importanza di uno scambio di informazioni senza ostacoli, che si svolga in maniera inclusiva e non discriminatoria.

Il Consiglio mette inoltre in evidenza i preziosi contributi del centro europeo di eccellenza per la lotta contro le minacce ibride di Helsinki e ne incoraggia la collaborazione con i pertinenti centri di eccellenza della NATO. Accoglie anche con favore gli scambi periodici e strutturati a livello del personale, che annoverano tra l'altro la cooperazione tra la cellula dell'UE per l'analisi delle minacce ibride, istituita all'interno del Centro dell'UE di analisi dell'intelligence (INTCEN), e la sezione della NATO per l'analisi delle minacce ibride.

10. Il Consiglio riconosce gli sforzi compiuti dagli Stati membri, in collaborazione con la Commissione e il servizio europeo per l'azione esterna (SEAE), nel condurre lo studio sui rischi ibridi previsto dall'azione 1 del quadro congiunto per contrastare le minacce ibride (del 2016) e chiede la prosecuzione dei lavori oltre a un'eventuale revisione dello studio in questione per accertare con maggior precisione le vulnerabilità.

Agire in modo coerente per rafforzare la resilienza e contrastare le minacce ibride

11. Per quanto riguarda lo sviluppo e l'utilizzo delle tecnologie nuove ed emergenti, che comprendono anche l'intelligenza artificiale e le tecniche di raccolta dei dati, occorre tenere in debito conto le nuove opportunità destinate a rafforzare la resilienza come pure le possibili vulnerabilità e gli effetti a cascata nel contesto del contrasto delle minacce ibride, allo scopo di ridurre i rischi globali, anche nel processo di pianificazione strategica del programma quadro di ricerca e innovazione.

12. Il Consiglio constata che le minacce ibride possono comportare attività informatiche dolose e, al riguardo, sottolinea la pertinenza del pacchetto di strumenti della diplomazia informatica dell'UE.

13. Il rapporto tra minacce ibride e sicurezza economica è un elemento pertinente che va preso in conto e che rimane principalmente responsabilità degli Stati membri.

14. È necessario impiegare in modo efficace i nuovi strumenti, quali il meccanismo previsto dal regolamento dell'UE sul controllo degli investimenti esteri diretti, per rafforzare la resilienza e contrastare le minacce ibride, in quanto offrono i mezzi di identificazione e di risposta agli investimenti esteri diretti che potrebbero incidere sulla sicurezza o sull'ordine pubblico.

15. Il Consiglio invita la Commissione a includere la resilienza nei confronti delle minacce ibride nel processo di valutazione di impatto per le future proposte legislative in materia, ivi compresi i futuri programmi quadro di ricerca e innovazione.

16. Il Consiglio sottolinea l'importanza di condurre esercitazioni periodiche e discussioni basate su possibili scenari relativamente al contrasto delle minacce ibride a livello ministeriale e ad altri livelli, come anche di includere elementi ibridi nelle altre attività di addestramento ed esercitazione dell'UE in materia a tutti i differenti livelli, con il sostegno degli Stati membri e degli organi pertinenti, in particolare il centro europeo di eccellenza per la lotta contro le minacce ibride, in funzione delle esigenze.

17. Allo scopo di garantire la coerenza delle prossime iniziative della cooperazione UE sul rafforzamento della resilienza e il contrasto delle minacce ibride, il Consiglio invita la Commissione e l'Alto rappresentante a mappare in modo esaustivo le misure adottate finora e i pertinenti documenti adottati nella prospettiva di eventuali nuove iniziative.

Nesso fra sicurezza interna ed esterna

18. Le autorità responsabili del contrasto, quelle incaricate della protezione civile e altre con competenze pertinenti dovrebbero continuare a sviluppare la loro preparazione per quanto riguarda la prevenzione e il contrasto delle minacce ibride. La cooperazione tra le autorità nazionali competenti e le istituzioni, gli organi e le agenzie dell'UE che si collocano lungo tutto lo spettro del nesso "sicurezza interna ed esterna", sulla base dei rispettivi mandati, dev'essere continuamente migliorata e integrata, aumentando nel contempo le sinergie e evitando una duplicazione degli sforzi, tra l'altro attraverso metodi di lavoro orizzontali, scambi volontari di informazioni e addestramento e esercitazioni intersettoriali. A tal fine, i ruoli di sostegno e i contributi forniti dai pertinenti meccanismi e agenzie dell'UE, nell'ambito dei rispettivi mandati e nel rispetto degli attuali vincoli di bilancio, dovrebbero essere ulteriormente valutati.

19. Occorre che le istituzioni e gli organi dell'UE, insieme con gli Stati membri, precisino ulteriormente l'uso dei pertinenti meccanismi e strumenti dell'UE a sostegno delle risposte degli Stati membri alle minacce intersettoriali e transfrontaliere, tra i quali rientrano i dispositivi integrati dell'UE per la risposta politica alle crisi (IPCR) e il meccanismo unionale di protezione civile (UCPM) con il suo Centro di coordinamento della risposta alle emergenze (ERCC).

20. Il Consiglio riconosce agli Stati membri la possibilità di invocare l'applicazione della clausola di solidarietà (articolo 222 del TFUE) per far fronte a una crisi grave provocata da un'attività di tipo ibrido.

Conoscenza situazionale e analisi dell'intelligence

21. La cooperazione unionale sul rafforzamento della resilienza e il contrasto delle minacce ibride dev'essere guidata da una valutazione della minaccia regolarmente aggiornata e da una conoscenza situazionale completa. Queste devono essere sviluppate dall'INTCEN dell'UE e dalla sua cellula per l'analisi delle minacce ibride allo scopo di rafforzare la capacità dell'UE e degli Stati membri di individuare, prevenire e contrastare le attività ibride, e di darvi risposta, sempre nel rispetto delle competenze degli Stati membri. Il Consiglio è del parere che occorra rafforzare ancor più le attività della cellula per l'analisi delle minacce ibride, contemplando un livello adeguato di risorse, anche per quanto riguarda le competenze professionali.

22. Il Consiglio rammenta le sue conclusioni sul contrasto alle minacce ibride del 19 aprile 2016, in cui chiedeva di mobilitare gli strumenti dell'UE per prevenire e contrastare le minacce ibride a carico dell'Unione e dei suoi Stati membri nonché dei partner. Il Consiglio sottolinea la necessità di sviluppare ulteriormente le attuali funzioni degli Stati membri e dell'UE in tema di conoscenza situazionale, tenuto conto delle fonti di minaccia, e di impiegare meglio l'analisi dell'intelligence dell'INTCEN dell'UE e della sua cellula per l'analisi delle minacce ibride, specie nei processi unionali di definizione delle politiche e di gestione delle crisi per quanto riguarda il contrasto delle minacce ibride.

23. Il Consiglio riconosce che le missioni e operazioni PSDC potrebbero fornire un contributo pertinente, se del caso, per l'identificazione e l'analisi degli indicatori di possibili azioni ibride di terzi, tra cui la disinformazione tendente a screditare e ostacolare l'azione dell'UE e degli Stati membri, e indica l'utilità di continuare ad esplorare la possibilità di sviluppare detto contributo.

Protezione delle infrastrutture critiche

24. La protezione delle infrastrutture critiche, nazionali ed europee, nonché delle funzioni e dei servizi cruciali per il corretto funzionamento dello Stato, dell'economia e della società è una priorità fondamentale, anche nell'ambito del rafforzamento della resilienza alle minacce ibride, cui deve dedicarsi tutta l'amministrazione e l'intera società. Questo approccio deve tenere in conto le forti interdipendenze tra i diversi servizi e funzioni critici, ivi compresi i servizi finanziari, il ruolo fondamentale del settore privato, il mutato contesto della sicurezza e i rischi emergenti, sotto il profilo sia materiale che informatico.

25. Vanno promosse inoltre, in aggiunta ai requisiti unionali e nazionali in campo giuridico, regolamentare e di vigilanza cui sono improntate la resilienza e la continuità operative, le intese con i responsabili del settore privato e gli operatori di servizi e infrastrutture, allo scopo di garantire la continuità dei servizi cruciali, e l'accesso ai medesimi, anche oltre i casi di "force majeure", assicurando un livello accettabile di preparazione per rispondere a tutte le minacce pertinenti e la flessibilità necessaria ad affrontare, mitigare e recuperare in seguito ad eventi scarsamente probabili ma ad elevato impatto.

26. Il Consiglio sottolinea che se la responsabilità della protezione delle infrastrutture critiche è principalmente una questione di competenza nazionale, il livello elevato di interdipendenze transfrontaliere e intersettoriali richiede sforzi coordinati o, se necessario, armonizzati a livello dell'UE, anche alla luce del funzionamento ininterrotto del mercato interno.

27. A seguito della valutazione, del luglio 2019, dell'attuazione della direttiva (2008/114/CE) relativa all'individuazione e alla designazione delle infrastrutture critiche europee, il Consiglio invita la Commissione a consultarsi con gli Stati membri in merito a un'eventuale proposta di revisione della direttiva da effettuare prontamente nel nuovo ciclo legislativo, che comprenda possibili misure aggiuntive volte a rafforzare la protezione e la resilienza delle infrastrutture critiche dell'UE, tenuto conto delle forti interdipendenze tra funzioni e servizi critici.

28. Il Consiglio invita la Commissione a continuare a dialogare con gli Stati membri e, ove opportuno, a sviluppare intese di cooperazione non vincolanti tra gli Stati membri che condividono infrastrutture critiche connesse.

29. Il Consiglio riconosce l'importanza della direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS) per lo sviluppo di una cultura di gestione del rischio e della sicurezza da parte degli operatori nei settori critici, oltre che per le capacità e strategie degli Stati che garantiscono un livello elevato di sicurezza delle reti e dei sistemi informativi nei rispettivi territori, anche sotto il profilo delle minacce ibride. Il Consiglio invita gli Stati membri, la Commissione e l'agenzia dell'Unione europea per la cibersicurezza (ENISA) a continuare a sviluppare la collaborazione sulla scorta della raccomandazione della Commissione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (il "programma") a tutti i livelli pertinenti.

Combattere la disinformazione e garantire elezioni libere e regolari

30. Il Consiglio accoglie con favore la relazione sull'attuazione del piano d'azione contro la disinformazione e riconosce che la prosecuzione dell'attuazione del piano d'azione resta al centro degli sforzi dell'UE. Il Consiglio sottolinea la necessità di riesaminare periodicamente il piano d'azione, aggiornandolo quando necessario, allo scopo di garantire un approccio efficace a lungo termine.

31. Il Consiglio sottolinea che l'azione della divisione per la comunicazione strategica del SEAE e in particolare delle tre task force (est, Balcani occidentali e sud) va sostenuta con risorse sufficienti che permettano una pianificazione, attuazione e valutazione a lungo termine. Tra i compiti che svolgono, le tre task force dovrebbero poter individuare, analizzare e contrastare, in modo continuativo, le attività di disinformazione da parte di attori di Stati stranieri e di attori non statali esterni. Le task force dovrebbero anche continuare a contribuire a una comunicazione efficace, positiva e basata sui fatti e alla promozione dei principi, dei valori e delle politiche dell'Unione nel vicinato orientale e meridionale dell'UE e nei Balcani occidentali, oltre che al rafforzamento dell'ambiente mediatico generale e della società civile nelle stesse regioni. Il Consiglio invita il SEAE a valutare la necessità e le possibilità di rafforzare la sua azione di comunicazione strategica in altre zone geografiche, ad esempio l'Africa subsahariana, mantenendo nel contempo la capacità necessaria a svolgere gli attuali compiti di comunicazione strategica.

32. Il Consiglio riconosce che un approccio globale a tutti i livelli si impone per far fronte alle sfide connesse alla disinformazione, che comprendono anche le interferenze miranti a compromettere lo svolgimento libero e regolare delle elezioni europee, utilizzando al meglio tutti gli strumenti disponibili online e offline. Detto approccio deve includere il monitoraggio e l'analisi delle interferenze a scopo disinformativo e manipolativo, il rispetto concreto delle norme europee in materia di protezione dei dati, l'applicazione delle salvaguardie elettorali, gli sforzi tesi a potenziare la pluralità dei media, il giornalismo professionale e l'alfabetizzazione ai social media, nonché la sensibilizzazione dei cittadini. Il Consiglio raccomanda di continuare a consolidare una rete attiva, indipendente e paneuropea di verificatori di fatti e di ricercatori contro la disinformazione.
Il Consiglio riconosce l'importanza e il ruolo della società civile, del mondo accademico e del settore privato nella lotta alla disinformazione e nello sviluppo della resilienza.

33. Il Consiglio riconosce il potenziale offerto dal sistema di allarme rapido (RAS) per quanto riguarda la lotta alla disinformazione, soprattutto in tema di interferenze elettorali. Sollecita la Commissione e il SEAE, insieme con gli Stati membri, a sviluppare ulteriormente il RAS affinché diventi una piattaforma generale che permette a Stati membri e istituzioni dell'UE di potenziare la cooperazione, il coordinamento e lo scambio di informazioni, quali ad esempio ricerca e conoscenze analitiche, migliori prassi e prodotti di comunicazione, a sostegno della lotta contro le campagne di disinformazione nell'ambito di uno strumentario di sforzi europei e nazionali.

34. Il Consiglio sottolinea l'utilità delle misure e delle raccomandazioni presentate dalla Commissione il 12 settembre 2018 nel suo pacchetto elettorale per la messa in sicurezza delle elezioni europee. Incoraggia la Commissione e gli Stati membri a sondare le possibilità di continuare le attività delle reti europee di cooperazione in materia elettorale in appoggio allo scambio di informazioni e migliori prassi. Il Consiglio si compiace degli sforzi compiuti dalla Commissione per coinvolgere tutti i soggetti interessati e sostenere un'ampia gamma di misure quali l'esercitazione sulla cibersicurezza delle elezioni europee (EU ELEx19), tenuto conto delle competenze nazionali in questo campo.

35. Il Consiglio sottolinea la necessità di continuare a colloquiare con le piattaforme dei social media allo scopo di conseguire standard più elevati di responsabilità, trasparenza e rendicontabilità per quanto riguarda la disinformazione. Oltre a ciò, è necessario accordare un accesso senza restrizioni ai dati anonimizzati dei fornitori di piattaforme dei social media a fini di ricerca accademica, onde favorire politiche basate sui fatti. Il Consiglio invita la Commissione a presentare iniziative sul modo di procedere in futuro per contrastare la disinformazione sulle piattaforme online. Tali iniziative dovrebbero fondarsi su una valutazione dell'attuazione del codice di buone pratiche sulla disinformazione, valutazione che dovrebbe tener conto del lavoro analitico e delle relazioni ad opera del mondo accademico e delle organizzazioni della società civile, della relazione di monitoraggio del codice elaborata dal gruppo dei regolatori europei per i servizi di media audiovisivi e anche degli insegnamenti tratti in seguito alle elezioni del Parlamento europeo di maggio 2019. In questo ambito, il Consiglio invita la Commissione a prendere in esame la maniera, ivi compresi possibili meccanismi di imposizione per le piattaforme online, di rafforzare maggiormente l'attuazione del codice di buone pratiche, in particolare includendo una valutazione indipendente sul rispetto, da parte dei firmatari, degli impegni da essi sottoscritti.

Sicurezza delle istituzioni, degli organi e delle agenzie dell'UE

36. La sicurezza del personale, delle istituzioni, degli organi e delle agenzie dell'UE nei confronti delle minacce ibride e di altre attività dolose è un interesse condiviso dall'UE e dai suoi Stati membri. Il Consiglio chiede alle istituzioni, agli organi e alle agenzie dell'UE, con il sostegno dagli Stati membri, di assicurare la capacità dell'Unione di proteggere la propria integrità e di rafforzare la sicurezza delle reti di informazione e comunicazione e dei processi decisionali dell'UE rispetto alle attività dolose di ogni genere, partendo da una valutazione completa delle minacce. A questo fine occorre che le istituzioni, gli organi e le agenzie, con il sostegno degli Stati membri, elaborino e mettano in pratica un insieme completo di misure destinate a garantirne la sicurezza, conformemente al mandato del Consiglio europeo di giugno 2019. Il Consiglio sottolinea l'importanza di assicurare l'interoperabilità dell'infrastruttura informatica dell'UE per lo scambio di informazioni classificate tra le istituzioni, gli organi e le agenzie dell'UE e gli Stati membri.