COMMISSIONE
EUROPEA

ALTO RAPPRESENTANTE
DELL'UNIONE PER
GLI AFFARI ESTERI E
LA POLITICA DI SICUREZZA

Bruxelles, 13.6.2018
JOIN(2018) 16 final

COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO, AL CONSIGLIO EUROPEO E AL CONSIGLIO

Rafforzamento della resilienza e potenziamento delle capacità di affrontare minacce ibride

1. INTRODUZIONE

Le attività ibride di soggetti statali e non statali continuano a rappresentare una seria e grave minaccia per l'UE e i suoi Stati membri. Le azioni volte a destabilizzare i paesi minando la fiducia dei cittadini nelle istituzioni pubbliche e sfidando i valori fondamentali della società sono diventate più frequenti. Le nostre società si trovano ad affrontare una grande sfida, posta da coloro che tentano di danneggiare l'Unione europea e i suoi Stati membri e che agiscono - tra l'altro - tramite attacchi informatici in grado di perturbare l'economia e i servizi pubblici, campagne di disinformazione mirate e azioni militari ostili.

Le campagne ibride sono multidimensionali e mirano a destabilizzare l'avversario combinando misure coercitive e sovversive e avvalendosi di strumenti e tattiche convenzionali e non convenzionali (di tipo diplomatico, militare, economico e tecnologico). Tali campagne, che possono essere utilizzate da soggetti sia statali che non statali, sono progettate in modo tale che risulti difficile individuarle o risalire al loro autore. L'attacco con agenti nervini del marzo scorso a Salisbury[1] ha evidenziato ulteriormente la versatilità delle minacce ibride e la moltitudine di tattiche attualmente disponibili. Il Consiglio europeo[2] ha risposto sottolineando la necessità di potenziare la capacità dell'Unione europea e dei suoi Stati membri di individuare, prevenire e rispondere alle minacce ibride in ambiti quali l'informatica, la comunicazione strategica e il controspionaggio. Esso ha inoltre richiamato l'attenzione in particolare sulla necessità di essere resilienti di fronte alle minacce connesse all'uso di sostanze chimiche, biologiche, radiologiche e nucleari.

Le minacce poste dalle armi non convenzionali fanno parte di una categoria a sé stante a causa della potenziale portata dei danni che ne possono derivare. Oltre a essere difficile individuarle e attribuirle, contrastare queste minacce rappresenta anche un problema complesso. Anche le minacce connesse all'uso di sostanze chimiche, biologiche, radiologiche e nucleari, che vanno al di là delle minacce ibride e riguardano anche le minacce terroristiche, generano una preoccupazione diffusa nella comunità internazionale[3], in particolare in relazione all'evoluzione del rischio di proliferazione, dal punto di vista geografico e tra i soggetti non statali.

Spetta innanzi tutto agli Stati membri rafforzare la resilienza a tali minacce e potenziare le capacità. Ad ogni modo, le istituzioni dell'UE hanno già intrapreso una serie di misure per contribuire a intensificare gli sforzi nazionali. Fra queste misure figura la stretta collaborazione con altri soggetti internazionali, in particolare con l'Organizzazione del trattato del Nord Atlantico (NATO)[4], che potrebbe divenire più intensa e portare all'assistenza agli Stati membri in ambiti quali l'intervento rapido[5].

---

1 Per quanto riguarda l'attacco di Salisbury, il 22 marzo 2018 il Consiglio europeo "ha concordato con la valutazione del governo del Regno Unito secondo cui è altamente probabile che la Federazione russa sia responsabile e che non vi sia una spiegazione alternativa plausibile."

2 Conclusioni del Consiglio europeo del marzo 2018.

3 Anche da parte del Consiglio di sicurezza delle Nazioni Unite, Risoluzione S/RES/2325 (2016) del 14 dicembre 2016.

4 La lotta contro le minacce ibride è uno dei sette ambiti di cooperazione con la NATO descritti nella dichiarazione congiunta firmata a Varsavia nel luglio 2016 dal presidente del Consiglio europeo, dal presidente della Commissione europea e dal segretario generale della NATO.

5 Il G7, riunito in occasione di un vertice a Charlevoix nel giugno 2018, ha inoltre convenuto di sviluppare un meccanismo di risposta rapida per far fronte alle minacce per la democrazia: https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats/

La presente comunicazione congiunta è la risposta della Commissione all'invito rivoltole dal Consiglio europeo a proseguire su questa strada. Essa fa parte di un pacchetto più ampio che comprende anche l'ultima relazione sui progressi verso l'Unione della sicurezza[6], che fa il punto della situazione e presenta le prossime tappe nell'attuazione del piano d'azione CBRN (in campo chimico, biologico, radiologico e nucleare) dell'ottobre 2017[7], e la seconda relazione sullo stato di avanzamento[8] dell'attuazione delle 22 azioni del "Quadro congiunto per contrastare le minacce ibride: la risposta dell'Unione europea"[9].

2. LA RISPOSTA DELL'UE

La Commissione e l'Alto rappresentante si sono costantemente adoperati per potenziare le capacità dell'UE e fornire agli Stati membri un sostegno efficace nella lotta contro le minacce ibride e le minacce connesse all'uso di sostanze chimiche, biologiche, radiologiche e nucleari. Sono già stati conseguiti risultati tangibili in ambiti quali le comunicazioni strategiche, la consapevolezza situazionale, il rafforzamento della preparazione e della resilienza e il potenziamento della capacità di risposta alle crisi.

La task force East StratCom, istituita in seguito al Consiglio europeo del marzo 2015, ha guidato le attività di previsione, individuazione e contrasto della disinformazione originata da fonti esterne. Le analisi degli esperti e gli altri lavori pubblici della task force[10] hanno aumentato notevolmente la consapevolezza circa l'impatto della disinformazione ad opera della Russia. Negli ultimi due anni East Stratcom ha scoperto oltre 4 000 casi di disinformazione, molti dei quali deliberatamente volti a colpire l'Europa. La task force ha inoltre incentrato il suo lavoro sul miglioramento della diffusione di comunicazioni positive, con una maggiore sensibilizzazione dei paesi del vicinato orientale. A seguito di tale successo sono state create altre due task force con focalizzazioni geografiche diverse: una per i Balcani occidentali e la Task Force South specifica per i paesi di lingua araba.

Sono state prese misure importanti per creare le strutture necessarie per migliorare la consapevolezza situazionale e fornire assistenza nel processo decisionale. Nel 2016 è stata istituita la cellula per l'analisi delle minacce ibride all'interno del Centro dell'UE di analisi dell'intelligence del Servizio europeo per l'azione esterna. La cellula riceve ed esamina informazioni riservate e liberamente accessibili provenienti da diversi portatori di interessi e concernenti le minacce ibride. Ad oggi sono stati prodotti oltre 100 valutazioni e briefing, condivisi all'interno dell'UE e tra gli Stati membri per contribuire al processo decisionale dell'UE. La cellula per l'analisi delle minacce ibride interagisce strettamente con il Centro europeo di eccellenza per la lotta contro le minacce ibride, che ha sede a Helsinki. Istituito nell'aprile 2017 per incentivare il dialogo strategico e svolgere attività di ricerca e analisi sulle minacce ibride, il Centro di eccellenza si è oramai allargato a 16 paesi[11] e riceve l'appoggio costante dell'UE.

---

6 Quindicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza [COM(2018) 470 final].

7 COM(2017) 610 final.

8 Relazione congiunta sull'attuazione del quadro congiunto per contrastare le minacce ibride (luglio 2017-luglio 2018), JOIN(2018) 14 final.

9 JOIN(2016) 18 final.

10 Cfr. www.euvsdisinfo.eu

11 Degli attuali 16 membri, 14 sono Stati membri dell'UE: Danimarca, Estonia, Finlandia, Francia, Germania, Italia, Lettonia, Lituania, Paesi Bassi, Polonia, Regno Unito, Repubblica ceca, Spagna, Svezia. L'idea di creare il Centro di eccellenza è venuta dal Quadro congiunto per contrastare le minacce ibride. Il Centro è stato inoltre sostenuto attivamente dall'UE e dalla NATO nel quadro della loro cooperazione.

Sono stati compiuti anche importanti progressi nel rafforzare la preparazione e la resilienza, in particolare contro le minacce connesse all'uso di sostanze chimiche, biologiche, radiologiche e nucleari. Negli ultimi sei mesi sono stati fatti importanti progressi nell'individuazione delle lacune da colmare per quanto riguarda la preparazione in caso di incidenti di sicurezza in ambito chimico, biologico, radiologico e nucleare, in particolare in termini di capacità di rilevamento per contribuire a prevenire gli attacchi in tali ambiti. Su iniziativa della Commissione, un consorzio di esperti nazionali ha analizzato le lacune concernenti le apparecchiature di rilevamento per diversi scenari connessi ai rischi chimici, biologici, radiologici e nucleari. La relazione di analisi delle lacune è stata condivisa con gli Stati membri, il che ha consentito loro di adottare decisioni consapevoli in materia di strategie di rilevamento e di intraprendere misure operative per colmare le lacune individuate.

Questo lavoro è stato supportato da esercitazioni volte a verificare il grado di avanzamento. L'esercitazione parallela e coordinata del 2017 (PACE17) con la NATO ha permesso di mettere alla prova in modo dettagliato la capacità di risposta dell'UE alle crisi ibride su vasta scala. L'esercitazione, senza precedenti in quanto a portata, ha messo alla prova non soltanto il manuale tattico dell'UE per contrastare le minacce ibride ("UE Hybrid Playbook"), i diversi meccanismi di reazione dell'UE e la loro capacità di interagire in modo efficiente, ma anche l'interazione tra la risposta dell'UE alle minacce ibride e l'intervento della NATO. È in corso la pianificazione di un'esercitazione per il 2018, con l'intento di istituire una prassi annuale, ma anche di aiutare gli Stati membri a rafforzare la loro capacità di risposta alle crisi ibride.

Queste misure mostrano come i quadri strategici messi in atto dall'UE stiano dando i loro frutti: diversi quadri sono stati elaborati negli ultimi due anni per guidare e focalizzare l'intervento dell'UE.

Il "Quadro congiunto per contrastare le minacce ibride: la risposta dell'Unione europea"[12], dell'aprile 2016, ha incoraggiato un approccio a tutti i livelli di governo, con 22 settori d'intervento, per contribuire a contrastare le **minacce ibride** e promuovere la resilienza dell'UE e degli Stati membri, nonché quella dei partner internazionali. La maggior parte delle azioni definite nel quadro congiunto è incentrata sul miglioramento della consapevolezza situazionale e sulla creazione di resilienza, con una migliore capacità di reazione. Esse vanno dal potenziamento della capacità di analisi dell'intelligence dell'UE al rafforzamento della protezione delle infrastrutture critiche, dal miglioramento della cibersicurezza alla lotta contro la radicalizzazione e l'estremismo violento. Le minacce e gli attacchi informatici sono un'altra priorità del quadro congiunto. La seconda relazione sui progressi compiuti nell'attuazione del quadro congiunto, adottata parallelamente alla presente comunicazione congiunta, evidenzia i progressi tangibili compiuti in relazione a tali azioni e conferma il potenziamento e l'intensificazione degli sforzi dell'UE per contrastare le minacce ibride[13].

Per quanto riguarda la **cibersicurezza**, il 9 maggio 2018 è stata una data cruciale, in quanto era il termine ultimo per il recepimento, da parte di tutti gli Stati membri dell'UE, della prima serie di norme giuridicamente vincolanti a livello dell'UE in materia di cibersicurezza, ossia la direttiva sulla sicurezza delle reti e dei sistemi d'informazione. Si tratta di una parte importante del più ampio approccio illustrato nel settembre 2017 nella comunicazione *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*[14], che prevedeva una vasta gamma di misure concrete volte a dare un forte impulso alle strutture e alle capacità dell'UE in materia di cibersicurezza. La comunicazione era

---

13 Per la prima relazione di attuazione (luglio 2017): JOIN(2017) 30 final.

14 JOIN(2017) 450 final.

incentrata sulla costruzione della resilienza dell'UE agli attacchi informatici e sul rafforzamento della capacità dell'UE in materia di cibersicurezza, sulla definizione di una risposta efficace sul piano del diritto penale e sul rafforzamento della stabilità mondiale attraverso la cooperazione internazionale. Essa era accompagnata da una proposta di legge sulla cibersicurezza, volta a rafforzare il sostegno a livello dell'UE[15], ed è stata sostenuta da una serie di proposte da portare avanti fino all'attuazione (cfr. di seguito).

La **disinformazione** danneggia le nostre democrazie compromettendo la capacità dei cittadini di prendere decisioni consapevoli e di partecipare al processo democratico. Con l'avvento di internet, il volume e la varietà delle notizie accessibili ai cittadini sono aumentati in modo considerevole. Tuttavia, le nuove tecnologie possono essere utilizzate per diffondere disinformazione a livelli e con una velocità senza precedenti, e in modo estremamente mirato per instillare diffidenza e creare tensioni sociali. La comunicazione della Commissione dal titolo *Contrastare la disinformazione online*: *un approccio europeo*[16] ha definito un approccio europeo in risposta al problema della disinformazione esortando all'azione diversi portatori di interessi, in particolare le piattaforme online ma anche le imprese del settore dei media. Le azioni contemplate riguardano una vasta gamma di ambiti significativi, che includono una maggiore trasparenza, l'affidabilità e la responsabilità delle piattaforme online, processi elettorali più sicuri e solidi, la promozione dell'istruzione e dell'alfabetizzazione mediatica, il sostegno al giornalismo di qualità e la lotta contro la disinformazione attraverso la comunicazione strategica. Le prime misure concrete comprendono un codice di buone pratiche sulla disinformazione, che dovrà essere elaborato da un forum multipartecipativo sulla disinformazione, e una rete di verificatori di fatti da mettere in piedi prima dell'estate. Durante la prima riunione del forum, il 29 maggio 2018, sono state decise le azioni da intraprendere per adottare il codice nel luglio dello stesso anno. Entro fine 2018 la Commissione valuterà i progressi compiuti nell'affrontare il problema e deciderà in merito all'eventuale necessità di un ulteriore intervento in questo ambito. Le attività previste saranno coerenti con quelle della task force East StratCom e complementari ad esse.

Per quanto riguarda i rischi connessi all'uso delle sostanze **chimiche, biologiche, radiologiche e nucleari**, nel suo *piano d'azione* dell'ottobre 2017[17] la Commissione ha proposto 23 misure e azioni concrete volte a migliorare la protezione dei cittadini e delle infrastrutture nei confronti di queste minacce, anche attraverso una più stretta cooperazione tra l'Unione europea e i suoi Stati membri e con la NATO. Nell'ambito delle misure per realizzare l'Unione della sicurezza volte a migliorare la protezione e la resilienza nei confronti del terrorismo, la Commissione ha proposto un approccio preventivo basato sull'assunto che i rischi connessi all'uso di sostanze chimiche, biologiche, radiologiche e nucleari sono poco probabili ma in caso di attacco l'impatto sarebbe elevato e duraturo. Nel frattempo, l'attentato di Salisbury e la crescente preoccupazione per l'interesse e la capacità dei terroristi di utilizzare tali sostanze sia all'interno che all'esterno dell'UE[18] dimostrano che la minaccia rappresentata dalle sostanze CBRN è reale. Ciò conferma ulteriormente l'impellente necessità di attuare pienamente il piano d'azione. Il piano segue un approccio rivolto a tutte le categorie di rischio ed è incentrato su quattro obiettivi: ridurre l'accessibilità degli agenti chimici, biologici, radiologici e nucleari; assicurare una più solida preparazione agli incidenti di sicurezza connessi all'uso di sostanze chimiche, biologiche, radiologiche e nucleari e una migliore risposta agli stessi; creare collegamenti più forti tra la sicurezza interna ed esterna

15 COM (2017) 477, cfr. di seguito.
16 COM (2018) 236 final.
17 COM(2017) 610 final.
18 Relazione di Europol sulla situazione e l'evoluzione del terrorismo (TE-SAT) 2017, pag. 16, disponibile all'indirizzo www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. Cfr. anche le dichiarazioni del direttore generale dell'OPCW: www.globaltimes.cn/content/1044644.shtml.

nel settore CBRN con i principali partner dell'UE a livello regionale e internazionale; accrescere la consapevolezza circa i rischi connessi all'uso delle sostanze CBRN. Informazioni dettagliate sui progressi tangibili nell'attuazione del piano d'azione sono fornite nell'ultima relazione sullo stato di avanzamento dell'Unione della sicurezza, adottata parallelamente alla presente comunicazione congiunta.

Infine, per aumentare l'efficacia degli sforzi volti a contrastare le minacce ibride e rafforzare il messaggio di unità tra gli Stati membri dell'UE e gli alleati della NATO, la cooperazione nella lotta contro le minacce ibride è stata definita come un ambito chiave della **cooperazione UE-NATO**, come indicato nella *dichiarazione congiunta di Varsavia* del luglio 2016[19]. Quasi un terzo di tutte le attuali proposte comuni per la cooperazione è incentrato sulle minacce ibride[20]. Quest'anno si sta intensificando la cooperazione con le esercitazioni e il "manuale tattico dell'UE"[21] citati in precedenza.

3. INTENSIFICARE LA RISPOSTA ALLE MINACCE IN EVOLUZIONE

3.1. Consapevolezza situazionale - rafforzamento della capacità di individuare le minacce ibride

Gli sforzi volti a contrastare e rispondere alle minacce ibride devono essere sostenuti dalla capacità di individuare precocemente le fonti e le attività ibride dolose, interne ed esterne, e di comprendere i possibili legami tra eventi spesso apparentemente scollegati. A tal fine, è essenziale utilizzare tutti i flussi di dati disponibili, compresi i dati di intelligence liberamente accessibili.

La cellula per l'analisi delle minacce ibride istituita nell'ambito del Servizio europeo per l'azione esterna come punto di riferimento unico dell'UE per l'analisi di tali minacce è una risorsa importante, ma ha bisogno delle competenze necessarie per affrontare l'intera gamma di minacce ibride, incluse quelle connesse all'uso di sostanze chimiche, biologiche, radiologiche e nucleari, e il controspionaggio. L'ampliamento delle competenze consentirebbe di rafforzare il sostegno alle risposte dell'UE a eventuali crisi future offrendo prodotti di intelligence civile e militare più completi in questi ambiti specifici. Tali misure potrebbero essere integrate da azioni a livello di Stati membri per aumentare il contributo dei servizi nazionali alla cellula per l'analisi delle minacce ibride e rafforzare ulteriormente la capacità della rete di punti di contatto nazionali con tale cellula di trasmettere ed elaborare informazioni urgenti. Gli Stati membri potrebbero inoltre aumentare il contributo di intelligence dei servizi nazionali al Centro dell'UE di analisi dell'intelligence (INTCEN), al fine di consentire un'analisi più approfondita delle potenziali minacce.

[19] La dichiarazione firmata dal presidente Juncker, dal presidente Tusk e dal segretario generale della NATO Stoltenberg costituisce l'attuale base per la cooperazione UE-NATO.

[20] 15283/16 e 14802/17.

[21] SWD(2016) 227 final.

Tappe future

- L'Alto rappresentante intende ampliare la cellula dell'UE per l'analisi delle minacce ibride con competenze specialistiche per le minacce CBRN, il controspionaggio e l'analisi delle minacce informatiche. Gli Stati membri sono invitati a fornire maggiori contributi di intelligence alla cellula per l'analisi delle minacce ibride esistenti ed emergenti.

- La Commissione, in collaborazione con l'Alto rappresentante, porterà a termine i lavori sugli indicatori di vulnerabilità per consentire agli Stati membri di valutare meglio il potenziale delle minacce ibride nei diversi ambiti. Questo lavoro sosterrà anche l'analisi condotta dall'UE delle tendenze nel campo delle minacce ibride.

3.2. **Azioni rafforzate nei confronti delle minacce chimiche, biologiche, radiologiche e nucleari**

Il piano d'azione dell'ottobre 2017 per rafforzare la preparazione contro i rischi per la sicurezza di natura chimica, biologica, radiologica e nucleare definisce il quadro d'intervento per rafforzare la preparazione, la resilienza e il coordinamento a livello dell'UE. Le azioni contemplate dal piano comprendono una serie di misure intese ad aiutare gli Stati membri attraverso la messa in comune delle competenze e il potenziamento delle capacità perseguito in modo congiunto, lo scambio di conoscenze e di buone prassi e l'intensificazione della cooperazione operativa. Gli Stati membri e la Commissione devono collaborare per attuare pienamente e con urgenza il piano d'azione. Inoltre, sulla scia dei progressi già compiuti in relazione all'analisi delle lacune in termini di capacità di rilevamento e allo scambio delle migliori prassi nell'ambito del gruppo di consulenza in ambito CBRN costituito di recente, l'Unione dovrebbe ora adottare ulteriori misure per far fronte alle minacce emergenti e in evoluzione. Ciò vale in particolare per le minacce chimiche. Sulla scorta delle iniziative già intraprese per limitare l'accesso ai precursori di esplosivi[22], l'Unione europea deve adottare rapidamente misure operative per controllare meglio l'accesso alle sostanze chimiche ad alto rischio e ottimizzare la capacità di individuare tali sostanze in una fase quanto più precoce possibile. Gli Stati membri dovrebbero inoltre prendere in considerazione lo svolgimento di ulteriori analisi delle lacune e di esercizi di mappatura a livello dell'UE, ad esempio in materia di resilienza alle minacce CBRN e di risorse e approcci per la decontaminazione. La preparazione a un attacco chimico, biologico, radiologico o nucleare e la gestione delle sue conseguenze richiedono il rafforzamento della cooperazione e del coordinamento tra gli Stati membri, comprese le autorità di protezione civile. Il meccanismo di protezione civile dell'Unione può giocare un ruolo chiave in tale processo allo scopo di rafforzare la capacità collettiva dell'Europa di prepararsi e di reagire.

[22] Nell'ambito del lavoro svolto nel quadro dell'Unione della sicurezza per ridurre il margine di manovra dei terroristi e dei criminali, la Commissione è intervenuta con decisione per ridurre l'accesso ai precursori di esplosivi che possono essere utilizzati per la fabbricazione di esplosivi artigianali. Nell'ottobre 2017 la Commissione ha presentato una raccomandazione in cui ha definito le misure immediate volte a prevenire l'uso improprio dei precursori di esplosivi sulla base delle norme esistenti (raccomandazione C(2017) 6950 final). Partendo da questa base, la Commissione ha adottato, nell'aprile 2018, una proposta volta a rivedere e rafforzare l'attuale regolamento (UE) n. 98/2013 relativo all'immissione sul mercato e all'uso di precursori di esplosivi [COM(2018) 209 final].

In tale ambito riveste particolare importanza anche la cooperazione internazionale, e l'UE può sfruttare i legami con i centri di eccellenza regionali in campo CBRN, anche cercando sinergie con la NATO, e i programmi di prevenzione, preparazione e reazione alle catastrofi naturali e provocate dall'uomo per le regioni meridionali e orientali[23].

Azioni future

- L'UE dovrebbe esaminare misure intese ad assicurare il rispetto delle regole e delle norme internazionali che combattono l'uso delle armi chimiche, anche attraverso un eventuale regime di sanzioni dell'UE per punire il ricorso a tali armi.
- Al fine di portare avanti il piano d'azione CBRN, la Commissione collaborerà con gli Stati membri per portare a termine le seguenti azioni entro la fine del 2018:
  - redigere un elenco di sostanze chimiche che rappresentano una specifica minaccia, che serva da base per l'intervento operativo volto a ridurre l'accessibilità alle stesse;
  - instaurare un dialogo con soggetti privati della catena di approvvigionamento ai fini di una collaborazione volta ad affrontare le minacce in evoluzione rappresentate dalle sostanze chimiche che possono essere utilizzate come precursori;
  - accelerare il riesame degli scenari di minaccia e l'analisi dei metodi di rilevamento esistenti, al fine di migliorare il rilevamento delle minacce chimiche, con l'obiettivo di sviluppare orientamenti operativi intesi ad esortare gli Stati membri a rafforzare le loro capacità di rilevamento.
- Gli Stati membri dovrebbero compilare inventari delle scorte di contromisure mediche essenziali, dei laboratori, delle cure e di altri mezzi. La Commissione collaborerà con gli Stati membri per mappare la disponibilità di tali scorte in tutta l'UE, al fine di renderle più facilmente accessibili e consentirne la rapida distribuzione in caso di attacchi.

3.3. **Comunicazione strategica - coerenza nella diffusione delle informazioni**

Una sfida importante connessa alle minacce ibride consiste nel sensibilizzare ed educare il pubblico a distinguere l'informazione dalla disinformazione. Sulla base dell'esperienza acquisita con la task force East StratCom, il Centro europeo di eccellenza per la lotta contro le minacce ibride e altre iniziative della Commissione[24], la Commissione e l'Alto rappresentante continueranno a sviluppare e a rendere più professionali le capacità di comunicazione strategica dell'UE, assicurando sistematicamente l'interazione e la coerenza tra le strutture esistenti. Queste iniziative saranno estese ad altre istituzioni dell'UE e agli Stati membri, anche mediante l'annunciata piattaforma online sicura sulla disinformazione.

[23] Nei paesi del vicinato orientale e meridionale la protezione civile organizza attività di formazione ed esercitazioni nell'ambito dei programmi di prevenzione, preparazione e risposta alle catastrofi naturali e provocate dall'uomo.

[24] Le rappresentanze della Commissione, ad esempio, sono attive anche sul fronte della verifica dei fatti e dei miti da sfatare. Diverse rappresentanze hanno sviluppato strumenti adattati alle realtà locali, come *Les Décodeurs de l'Europe* in Francia, "UE Vero Falso" in Italia, un concorso pubblico in Austria per i cartoni animati sui miti da sfatare concernenti l'UE, un'analoga serie di cartoni animati in Romania ed Euromyths A-Z nel Regno Unito. Altri progetti di questo tipo sono in corso di sviluppo.

Il miglioramento del coordinamento e della cooperazione in materia di comunicazione strategica in tutte le istituzioni dell'UE, con gli Stati membri e con i partner e le organizzazioni internazionali sarà essenziale e richiede preparazione e pratica prima di poter rispondere alle crisi in tempo reale.

I periodi elettorali si sono rilevati bersagli particolarmente strategici e sensibili per gli attacchi informatici e l'elusione online delle misure di sicurezza convenzionali ("offline") e di regole come il periodo di silenzio, norme trasparenti in materia di finanziamento e parità di trattamento dei candidati. Gli attacchi hanno preso di mira anche le infrastrutture elettorali e i sistemi informatici utilizzati nelle campagne elettorali; inoltre, alcuni paesi terzi hanno condotto campagne di disinformazione online di massa di matrice politica e sferrato attacchi informatici con l'intento di screditare e delegittimare le elezioni democratiche. A livello dell'UE si stanno portando avanti diversi filoni di attività per sensibilizzare gli Stati membri nella preparazione e nella reazione a queste minacce in costante evoluzione. In sede di Consiglio, le autorità degli Stati membri incaricate della cibersicurezza[25] emaneranno orientamenti volontari e definiranno buone prassi comuni per far fronte ai problemi connessi alla cibersicurezza delle tecnologie utilizzate nei periodi elettorali per l'intera durata degli stessi. Tali tecnologie comprendono i sistemi informatici e le soluzioni TIC utilizzate per la registrazione di elettori e candidati, la raccolta e il conteggio dei voti e la diffusione dei risultati, come pure i sistemi ausiliari direttamente connessi alla legittimità dei risultati elettorali.

In caso di attacchi ibridi è inoltre necessario fornire al pubblico informazioni affidabili e coerenti in tempi rapidi. Gli incidenti connessi all'uso di sostanze chimiche, biologiche, radiologiche e nucleari e gli eventi che possono avere un impatto analogo generano forti proteste tra i cittadini, che chiedono risposte rapide. I messaggi strategici svolgono un ruolo fondamentale, anche tra le organizzazioni internazionali che potrebbero essere in procinto di adottare separatamente i loro piani di reazione.

Azioni future

- Il Servizio europeo per l'azione esterna e la Commissione collaboreranno nell'ambito delle rispettive competenze al fine di instaurare una cooperazione più strutturata in materia di comunicazioni strategiche per far fronte al problema della disinformazione originata all'interno e all'esterno dell'UE e scoraggiare la produzione di disinformazione ostile e le interferenze ibride da parte di governi stranieri.

- Nell'autunno la Commissione organizzerà eventi ad alto livello con gli Stati membri e i pertinenti portatori di interessi, compreso il convegno sui diritti fondamentali dedicato alla democrazia, al fine di promuovere buone prassi e orientamenti su come prevenire e attenuare le minacce in contesto elettorale basate sull'uso degli strumenti informatici e della disinformazione e su come reagire alle stesse.

- L'Alto rappresentante e la Commissione valuteranno come sostenere nel modo migliore, fornendo strumenti e risorse, il lavoro svolto dalle tre task force StratCom per fare in modo che gli sforzi dell'UE siano sufficientemente intensificati per far fronte alla complessità delle campagne di disinformazione condotte da soggetti ostili.

[25] Sotto l'egida del gruppo di cooperazione istituito a norma della direttiva sulla sicurezza delle reti e dei sistemi d'informazione.

3.4. **Potenziamento della resilienza e dissuasione nel settore della cibersicurezza**

La cibersicurezza è essenziale sia per la nostra prosperità che per la nostra sicurezza. Vista la crescente dipendenza della nostra vita quotidiana e delle nostre economie dalle tecnologie digitali, siamo sempre più esposti.

L'efficacia della cibersicurezza nell'UE oggi è ostacolata da investimenti e coordinamento insufficienti. L'UE sta cercando di far fronte a questo problema sviluppando le capacità tramite misure di sostegno, un maggiore coordinamento e nuove strutture per far progredire le tecnologie di cibersicurezza e favorirne la diffusione[26]. La direttiva sulla sicurezza delle reti e dei sistemi informativi[27] ha introdotto un livello minimo di sicurezza delle reti e dei sistemi informativi in tutta l'Unione. La sua piena attuazione da parte di tutti gli Stati membri è essenziale per migliorare la ciberresilienza: si tratta di un primo passo fondamentale. Il regolamento generale sulla protezione dei dati introduce l'obbligo di notificare all'autorità di vigilanza competente la violazione dei dati personali. Altre misure fondamentali includono un'Agenzia dell'Unione europea per la cibersicurezza rafforzata e modernizzata e un quadro dell'UE in materia di certificazione dei prodotti e servizi TIC[28] per conquistare la fiducia dei consumatori. Sono in corso anche attività volte a fornire assistenza alla rete di centri di competenza degli Stati membri per incoraggiare lo sviluppo e la diffusione delle soluzioni di cibersicurezza e integrare gli sforzi di sviluppo delle capacità in questo ambito a livello nazionale e dell'UE. Tali attività si baseranno sul lavoro del programma Europa digitale presentato dalla Commissione il 6 giugno[29], che attribuisce una nuova priorità agli investimenti dell'UE in cibersicurezza.

Al tempo stesso, una raccomandazione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (il "programma")[30] ha stabilito le modalità della cooperazione tra gli Stati membri e vari soggetti dell'UE nella risposta agli attacchi informatici transfrontalieri su vasta scala. Essa ha sottolineato il ruolo essenziale della consapevolezza situazionale ai fini di un coordinamento efficace a livello tecnico, operativo e strategico/politico. Il gruppo di cooperazione istituito a norma della direttiva sulla sicurezza delle reti e dei sistemi informativi si sta inoltre adoperando per migliorare lo scambio e la condivisione delle informazioni fra le parti interessate, attraverso lo sviluppo di una tassonomia comune per la descrizione degli incidenti. Questo approccio sarà sperimentato durante le prossime esercitazioni. L'analisi strategica delle minacce informatiche attuali ed emergenti, basata sui contributi dei servizi di intelligence degli Stati membri, è fornita dalla cellula per l'analisi delle minacce ibride.

Il quadro relativo a una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica") è stato un importante passo avanti in termini operativi, che ha delineato le misure da varare nell'ambito della politica estera e di sicurezza comune, comprese misure restrittive alla quali ricorrere per rafforzare la risposta dell'UE ad attività che ne danneggiano gli interessi politici, di sicurezza ed economici. Quanto più gli Stati membri vi ricorreranno appieno, tanto maggiore sarà l'efficacia dissuasiva. Nel mese di aprile, il Consiglio "Affari esteri" ha adottato conclusioni sulle attività informatiche dolose in cui condanna con fermezza l'uso delle

---

[26] Nel quadro del rafforzamento dell'innovazione nelle regioni europee, nel dicembre 2017 è stata avviata una nuova azione pilota interregionale che riunisce le regioni dell'UE per intensificare le attività nel campo della cibersicurezza.

[27] Direttiva 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.

[28] COM(2017) 477 final.

[29] Proposta di regolamento che istituisce il programma Europa digitale per il periodo 2021-2027, COM(2018) 434.

[30] C(2017) 6100.

tecnologie dell'informazione e della comunicazione a scopo doloso, incluse quelle utilizzate negli attacchi Wannacry e NotPetya, che hanno causato gravi danni e perdite economiche nell'UE e al di fuori dei suoi confini.

L'Unione europea e i suoi Stati membri devono migliorare la loro capacità di individuare gli autori degli attacchi informatici, non da ultimo migliorando la condivisione dei dati di intelligence. La capacità di individuare i responsabili agirebbe da deterrente nei confronti dei potenziali aggressori e aumenterebbe le probabilità che i responsabili rendano conto delle proprie azioni. Aumentare l'effetto dissuasivo è un obiettivo fondamentale dell'approccio strategico della Commissione volto a rafforzare la cibersicurezza. Le recenti proposte della Commissione intese a migliorare la raccolta transfrontaliera di prove elettroniche da utilizzare nei procedimenti penali rafforzerebbe inoltre in misura significativa la capacità delle autorità di contrasto di indagare e perseguire la criminalità informatica.

Una forte ciberresilienza richiede un approccio collettivo e di vasta portata. Ciò richiede strutture più solide ed efficaci per promuovere la cibersicurezza e rispondere agli attacchi informatici negli Stati membri anche all'interno delle istituzioni, delle agenzie e degli organismi dell'UE: l'assenza di una rete di comunicazione sicura tra le istituzioni europee è un serio problema. Bisognerebbe accrescere la consapevolezza in materia di cibersicurezza nelle istituzioni dell'UE e da parte del loro personale migliorando la cultura della sicurezza e intensificando le attività di formazione.

Azioni future

- Il Parlamento europeo e il Consiglio dovrebbero accelerare i lavori per portare a termine i negoziati sulle proposte in materia di cibersicurezza per giungere a un accordo entro la fine dell'anno e trovare rapidamente un accordo sulla proposta legislativa sulla raccolta di prove elettroniche.

- La Commissione e l'Alto rappresentante collaboreranno strettamente con gli Stati membri per far progredire le attività relative agli aspetti informatici dei meccanismi di gestione delle crisi e risposta alle stesse a livello dell'UE. Gli Stati membri sono invitati a proseguire le attività relative all'individuazione degli autori degli attacchi informatici e all'utilizzo pratico degli strumenti di diplomazia informatica per intensificare la risposta politica agli attacchi informatici.

- In risposta alla necessità di rafforzare le nostre capacità di difesa informatica, è in corso la costituzione di una piattaforma dedicata di formazione e istruzione, che contribuirà a coordinare le opportunità di formazione sulla difesa informatica offerte dagli Stati membri. Saranno cercate sinergie con iniziative analoghe della NATO.

3.5. **Rafforzamento della resilienza alle attività di intelligence ostili**

La lotta contro le attività di intelligence ostili richiede innanzitutto e soprattutto un coordinamento efficace e rafforzato tra gli Stati membri, conformemente alle pertinenti norme e disposizioni dell'UE e nazionali. È tuttavia indispensabile anche rafforzare la capacità delle istituzioni dell'UE di contrastare la crescente minaccia rappresentata dalle attività di questo tipo dirette specificamente alle istituzioni e creare una cultura di sensibilizzazione alla sicurezza, supportata da una formazione e da una sicurezza fisica migliori. Le istituzioni potrebbero inoltre collaborare con gli Stati membri per realizzare un sistema di accreditamento dell'UE più solido. Un tale sistema sarebbe basato sulla

comunicazione proattiva, in grado di consentire una maggiore consapevolezza tra gli Stati membri e le istituzioni circa gli eventuali soggetti ostili, in particolare quelli già individuati dagli Stati membri.

Il coordinamento tra gli Stati membri e tra questi ultimi e altre organizzazioni internazionali, in particolare la NATO, contribuirebbe a incrementare le attività di controspionaggio volte a contrastare le attività ostili nell'UE. Un esempio di ambito che trarrebbe beneficio da un maggiore coordinamento tra gli Stati membri è il controllo degli investimenti, sulla base di un regolamento[31] proposto nel settembre 2017 dalla Commissione per il controllo degli investimenti esteri diretti da parte degli Stati membri per motivi di sicurezza o di ordine pubblico. Un maggiore coordinamento tra gli Stati membri sarebbe altrettanto importante per controllare le operazioni finanziarie, poiché i servizi di intelligence ostili sempre più spesso finanziano le loro azioni contro l'UE attraverso elaborati sistemi finanziari.

Azioni future

- Il Servizio europeo per l'azione esterna e la Commissione attueranno misure pratiche migliorate per sostenere e sviluppare la capacità dell'UE di interagire con gli Stati membri per contrastare le attività di intelligence ostili dirette specificamente alle istituzioni.
- La cellula per l'analisi delle minacce ibride rafforzata sarà integrata con competenze in materia di controspionaggio per fornire analisi approfondite e note informative sulla natura delle attività di intelligence ostili dirette a colpire individui e istituzioni.
- Il Parlamento europeo e il Consiglio dovrebbero accelerare i lavori per portare a termine i negoziati sulla proposta relativa al controllo degli investimenti entro la fine dell'anno.

4. CONCLUSIONI

Le minacce ibride e le minacce connesse all'uso di sostanze chimiche, biologiche, radiologiche e nucleari sono state al centro delle preoccupazioni dell'UE. L'attacco sferrato a marzo nel Regno Unito ha messo in luce l'ampia varietà delle azioni intraprese nell'ambito della guerra ibrida e la necessità di una maggiore resilienza alle minacce CBRN.

La Commissione e l'Alto rappresentante hanno adottato e proposto una serie di iniziative per affrontare le sfide poste dalle minacce ibride. La Commissione sta inoltre accelerando l'attuazione del piano d'azione del 2017 per migliorare la preparazione contro i rischi per la sicurezza posti dagli attacchi con sostanze chimiche, biologiche, radiologiche e nucleari.

La presente comunicazione congiunta è intesa a informare il Consiglio europeo sulle attività in corso e a individuare gli ambiti in cui è opportuno intensificare gli sforzi al fine di approfondire ulteriormente e rafforzare il contributo essenziale dell'UE nella lotta contro queste minacce. Spetta ora agli Stati membri, alla Commissione e all'Alto rappresentante assicurare che venga dato un rapido seguito a tali azioni.

[31] Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione europea, COM(2017) 487.