Audizione Min. Plen. Laura Carpini (Capo Unità per le politiche dello spazio cibernetico del MAECI)

IV Commissione Senato della Repubblica, 25 luglio ore 12

1. Ringrazio per l'invito che mi consente di raccontare il ns lavoro su un tema relativamente nuovo per la diplomazia e al tempo stesso contribuire, proprio con la prospettiva diplomatico-geopolitica, al lavoro del Parlamento su un tema così attuale e importante per la sicurezza nazionale ed europea, quale la sicurezza cibernetica e i modi per rafforzarla.
2. Dal punto di vista del MAECI, quanto precede si declina lungo tre direttrici: a) il rafforzamento della protezione delle ns strutture; b) il contributo al negoziato sugli strumenti europei nel gruppo consiliare HWPCI insieme all'ACN; c) il rafforzamento dell'azione diplomatica in campo internazionale su questo settore.
3. Per quanto riguarda il primo punto, il Ministro Tajani ha impresso un notevole impulso al rafforzamento della sicurezza della Farnesina e della rete estera, basti pensare che di recente ha nominato un Suo inviato speciale, il Min. Plen. Michele Giacomelli, di ciò incaricato e il 19 luglio è stato bandito un nuovo concorso a più profili, tra cui uno per funzionari informatici che andranno a rafforzare il contingente attuale;
4. Per quanto riguarda la seconda direttrice, dal punto di vista tecnico e degli strumenti che il Parlamento deve esaminare, la relazione che avete ricevuto dall'ACN è esaustiva e, dalla prospettiva dell'Unità che dirigo, non posso che sposarla. Interpreto dunque il mio contributo in questa audizione sottolineando alcuni aspetti che possono arricchire il materiale a disposizione, collocando questo processo nel quadro più ampio e in continua evoluzione quale quello che stiamo vivendo.
5. L'aggressione russa all'Ucraina ha impresso un'accelerazione drammatica e acuito il senso di urgenza del rafforzamento della postura di sicurezza cibernetica dell'UE e dei suoi Stati membri, innestandosi saldamente sul lavoro già avviato con la priorità della Commissione "A Europe fit for the digital age" e relativi strumenti. Il conflitto in Ucraina, seppur prevalentemente convenzionale e in qualche modo sconfessione degli esperti che preconizzavano guerre cibernetiche come il cigno nero dell'immediato futuro, ha reso evidenti alcuni aspetti dell'uso malevolo degli strumenti cyber:
    - L'azione malevola cyber, anche sotto soglia, come avviene nella maggior parte dei casi, come fattore abilitante di un conflitto armato (ViaSat e attacchi di indebolimento precedenti);
    - Il potenziale di spill over;
    - L'importanza dell'assistenza e del coordinamento in caso di attacchi su larga scala;
    - Il ruolo degli attori non statuali (settore privato ma non solo), sia in senso positivo sia in senso negativo;
    - L'uso di armi autonome, l'importanza delle comunicazioni satellitari e della sicurezza dell'ambiente cyber-digitale esteso.
6. Aggiungo che, secondo il rapporto sugli scenari di rischio redatto dall'Agenzia Europea per la Cybersicurezza (ENISA), all'avvio delle ostilità in Ucraina è corrisposto un significativo aumento delle azioni cyber ostili contro i governi che hanno manifestato sostegno a Kiev: nel solo 2022, ENISA indica in 128 le organizzazioni governative vittime di attacchi cyber in 42 paesi, con un focus principale tra gli Stati membri UE e NATO, gli Stati Uniti e i paesi confinanti con l'Ucraina).

7. Questi elementi, oltre a illustrare l'impatto della geopolitica sull'evoluzione della minaccia cyber, spiegano già da soli l'urgenza di accelerare il processo di rafforzamento della postura di sicurezza cybernetica europea.
8. Il senso è che in un ambiente altamente interconnesso e veloce come quello cyber, ogni compartimento stagno, strozzatura, interruzione o rallentamento, espone a rischi di propagazione di un attacco, diminuisce la capacità di prevenzione, di mitigazione e di assistenza da parte di altri Stati membri e/o di potenziali attori del settore privato in grado di aiutare.
9. Lo scorso 18 aprile, la Commissione ha dunque presentato il "Cyber Package", cioè il pacchetto di misure mirante a dare concreto seguito alle previsioni della Bussola Strategica e della più recente Comunicazione Congiunta sulla "Cyber Defence Policy (CDP)". Nello specifico, il Cyber Package si compone di tre pilastri: il "Cyber Solidarity Act" , gli emendamenti proposti al "Cyber Security Act" sulla certificazione della cybersicurezza dei servizi di sicurezza gestiti, nonché la "Cybersecurity Skills Academy", nel formato di una Comunicazione della Commissione.
10. Il "Cyber Solidarity Act" si articola lungo "detection", "preparedness" e "response" per la risposta solidale dell'UE e dei suoi Stati membri ad attacchi cyber considerevoli e su larga scala e punta alla creazione di:
11. a) uno "European Cyber Shield", vale a dire un'infrastruttura paneuropea di "Security Operation Centres (SOCs)" nazionali e regionali ("Cross-border SOCs") per il monitoraggio e l'avviso preventivo su imminenti attacchi cyber.
12. b) un "Cyber Emergency Mechanism", per incrementare il grado di preparazione e risposta agli incidenti cyber nell'UE, accompagnato da meccanismi di sostegno finanziario per la mutua assistenza tra Stati membri e la creazione di una riserva di servizi forniti da attori certificati del settore privato.
13. c) un "Cybersecurity Incident Review Mechanism" per valutare ed esaminare specifici incidenti di cybersicurezza.
14. In linea con quanto illustrato dall'ACN nella sua relazione, le proposte sono da salutare con favore, nel loro complesso e per i motivi suesposti. Come ACN, tuttavia, si ritiene che vi siano aspetti ancora da affinare, tra cui:
15. i servizi di sicurezza gestiti, le modalità di coinvolgimento dello European Cybersecurity Certification Group (ECCG), i rischi di duplicazione dell'attività dei SOCs nazionali con quanto realizzato dagli CSIRT nazionali; lo stesso dicasi per la rete di SOCs regionali, rispetto allo "CSIRT Network", la rete degli CSIRT nazionali UE o il Cybersecurity Incident Review Mechanism, rispetto al mandato attribuito a CyCLONe .
16. Per questi motivi, la discussione riprenderà a settembre su entrambi gli strumenti in Gruppo HWPCI, e la possibilità di raggiungere un compromesso si giocherà sulla linea di faglia tra prerogative nazionali ed esigenze di condivisione e cooperazione a livello UE, stante la natura orizzontale e pervasiva della dimensione cyber. La rilevanza politica della proposta è, in ogni caso, evidente, così come è evidente che ad essa si accompagnano interessanti opportunità di natura industriale per le imprese nazionali attive nel settore, data la mobilitazione importante di risorse finanziarie, non ultimo per acquisire, tramite procedure di appalto, le tecnologie, gli strumenti e i servizi necessari.
17. Vorrei concludere richiamando alcuni elementi della terza direttrice, l'azione propria della struttura – relativamente nuova – che dirigo al MAECI, la cosiddetta "diplomazia della sicurezza cibernetica". Nel fare le nostre scelte dobbiamo sempre tenere conto del quadro internazionale e geopolitico in cui ci muoviamo.
18. Il richiamo alle prerogative nazionali di tutela della sicurezza e dell'ordine pubblico nell'attuale dibattito sui regolamenti in esame, trova una sua ragion d'essere anche nelle implicazioni legali del comportamento degli Stati a livello internazionale, di quello delle

regolamentazioni europee a livello internazionale e nell'appartenenza del nostro e di molti altri Stati membri dell'UE alle Nazioni Unite, alla NATO e ad altre organizzazioni internazionali e regionali. Da un lato, un rafforzamento dell'integrazione e della regolamentazione europea in questo settore ha senz'altro un effetto positivo come modello per altre regioni che stanno cercando di rafforzare la collaborazione su questo tema, pur partendo da un livello di integrazione molto minore. Rafforzare un anello importante come l'UE in termini di resilienza, certezza delle procedure e capacità di mitigazione e assistenza contribuisce inoltre alla stabilità internazionale e al rafforzamento della cornice di comportamento responsabile degli Stati su cui stiamo lavorando da anni anche alle Nazioni Unite (è in corso l'Open Ended Working Group della Prima Commissione delle Nazioni Unite e stiamo lavorando da anni con i partners UE e like-minded per la creazione di un Programma di Azione sul comportamento responsabile degli Stati in ambito cyber).

19. D'altro canto, le prerogative nazionali esclusive devono essere protette, in mancanza di maggiori forme di integrazione, soprattutto quando si tratta di sicurezza e di comportamenti che possono avere impatti oltreconfine e/o comportare assunzione di responsabilità legale internazionale sia da parte dell'UE sia da parte degli Stati membri.

20. Il negoziato che riprenderà a settembre sarà dunque da seguire con attenzione ma sono certa che verrà trovato il punto di incontro soddisfacente. Si tratta infatti di un numero limitato di differenze di opinione su strumenti di valenza altamente positiva e urgente per tutta l'UE.