Mercoledì 13 giugno 2018 - 12:15

# Cyber security, I-Com: due i problemi principali a livello Ue

L'analisi contenuta nel nuovo Rapporto Osservatorio Innov-E 2018

Roma, 13 giu. (askanews) – Sono due "i problemi principali che bloccano una vera reazione a livello europeo alle minacce cibernetiche". È quanto si legge nel nuovo Rapporto Osservatorio Innov-E 2018 realizzato da I-Com – Istituto per la Competitività, presentato oggi a Roma.

"Il primo", prosegue il testo, "è la riluttanza a cedere sovranità in una materia così delicata che attiene anche e soprattutto a questioni di sicurezza nazionale. Un'armonizzazione delle normative, ma soprattutto una condivisione di informazioni tra Stati membri, diventa in questo modo più difficile e rende la governance della cybersecurity un'anatra zoppa. Nel 2016 l'Ue aveva pianificato di investire 1,8 miliardi di euro entro il 2020 come primo passo per superare frammentazione fra Paesi e arrivare a un maggior coordinamento delle strutture di risposta, ma la ritrosia a cedere sovranità potrebbe bloccare tali sforzi un po' come è successo ai tentativi di creazione di un'unica agenzia di intelligence europea".

Il secondo problema "non risolto", aggiunge l'analisi, "è la mancata compenetrazione di settore pubblico e privato nella gestione dei rischi cibernetici (Parlamento europeo, 2013). Nel 2009 si era cercato di istituire con la direttiva sulla protezione delle infrastrutture critiche lo European Public-Private Partnership for Resilience (EP3R), un tentativo di formalizzare un meccanismo di partnership pubblico-privata. Molto presto il consesso è diventato un forum di lobbying, con tentativi da parte del privato di influenzare la legislazione piuttosto che di cooperare con le istituzioni per formare nuovi standard di resilienza.

Oltretutto si registrò una disparità tra imprese dell'Ict e quelle delle infrastrutture, con le seconde nettamente sottorappresentate. Anche il tentativo di rivitalizzarla nel 2013 creando una nuova piattaforma non ha portato ai risultati sperati e l'interazione tra soggetti diversi per migliorare la risposta resta ancora difficile da realizzare".

Il cammino per risolvere queste e altre criticità, conclude lo studio, "è stato di fatto avviato nell'ultimo anno, con la nuova proposta del Cybersecurity Act nel settembre 2017 e con l'entrata in vigore della direttiva Gdpr e la trasposizione nell'ordinamento italiano della direttiva Rsi (nota anche come Nis, ndr). Un cammino che vuole superare il problema di frammentazione regolatoria e degli standard tecnici attraverso maggiore cooperazione e armonizzando i diversi approcci nazionali. Un'applicazione omogenea delle normative esistenti, unita all'impulso che potrebbe dare il sistema di certificazione europea, potrebbe costituire un punto di inizio per tenere conto di tutte le interdipendenze del sistema energetico a livello europeo e per far fronte a una minaccia intangibile, che però ha conseguenze estremamente reali".

(Fonte: Cyber Affairs)