INTERVISTA AD ANTONELLA COLONNA VILASI

DOMANDA 1)

Molti affiliati del Califfato sono giovani cresciuti in Occidente, non è escluso che abbiano la capacità di portare avanti operazioni del genere. Inoltre è ormai chiaro come l'Isis conosca molto bene il funzionamento dei social media e della rete, usata sia per fare propaganda, sia per reclutare. Sicuramente è stata un'altra vittoria mediatica per lo Stato islamico ed i suoi fiancheggiatori, capaci di inserirsi in uno dei sistemi più protetti del mondo. Questa dimensione totale del conflitto sarebbe stata impensabile ed ingestibile per un gruppo terroristico fino a qualche anno fa, l'ISIS però ha fatto un salto di qualità notevole. Alcuni messaggi di propaganda firmati dall'ISIS con la sigla "Cybercaliphate"sono stati inseriti da alcuni hacker nell' account Twitter e YouTube del Comando centrale delle Forze armate statunitensi (CENTCOM), inserendo frasi e video inneggianti al Califfato. Ed è la prima volta che una formazione jihadista utilizza tattiche di cyberwar contro account legati ad uno Stato. Se l'Isis possiede una squadra specializzata di hacker la sua connotazione di gruppo jihadista supera e deborda la sua essenza ed assume quella di "esercito". Questo attacco cibernetico è stato sferrato dall' ISIS pochi giorni dopo la strage di Charlie Hebdo, ma soprattutto mentre negli USA il presidente Obama annunciava il rafforzamento dei sistemi di sicurezza informatici. Gli hacker del Califfato hanno anche pubblicato documenti e piani militari statunitensi su Cina e Corea del Nord, tuttavia non di natura riservata. L'Fbi sta investigando sull'hackeraggio di alcuni account Twitter di giornali e tv private. Si tratta di operazioni di "deface", ossia di modifica delle pagine e del contenuto dei profili social, sui quali sono comparsi l'immagine di un uomo a volto coperto e la scritta "I love you Isis". Alcuni esperti ritengono che alcuni gruppi affermino di agire nel nome del jihad ma non siano assolutamente collegati con lo Stato Islamico.

DOMANDA 2)

L'insieme delle attività di preparazione e conduzione delle operazioni militari eseguite nel rispetto dei principi bellici condizionati dall'informazione. Si traduce nell'alterazione e addirittura nella distruzione dell'informazione e dei sistemi di comunicazioni nemici. La guerra cibernetica si caratterizza per l'uso di tecnologie elettroniche, informatiche e dei sistemi di telecomunicazione.

Gli attacchi informatici contro Paesi e le loro aziende stanno aumentando ultimamente in modo esponenziale.

Le regole base della guerra cibernetica sono:

- minimizzare la spesa di capitali e di energie produttive e operative;
- sfruttare appieno le tecnologie che agevolino le attività investigative e di acquisizione di dati, l'elaborazione di questi ultimi e la successiva distribuzione dei risultati ai comandanti delle unità operative;

- ottimizzare al massimo le comunicazioni tattiche, i sistemi di posizionamento e l'identificazione amico-nemico .

Ricordo il worm Stuxnet, un attacco informatico agli impianti nucleari iraniani che è stato attuato nel 2010, utilizzato da Israele e Stati Uniti, per danneggiare le centrifughe nucleari iraniane.

DOMANDA 3)

Il Cyber Command (USCYBERCOM) statunitense è un comando delle forze armate americane subordinato al Comando Strategico degli Stati Uniti . Il comando si trova a Fort Meade, nel Maryland , e centralizza tutte le operazioni di comando in materia di cyberspazio, gestisce le risorse informatiche esistenti e sincronizza le reti statunitensi di difesa militari. Il Cyber Command è composto da diverse strutture, le unità militari:

- Army Cyber Command / Second Army (Esercito)
    - Army Network Enterprise Technology Command / 9 ° Army Signal Command(NETCOM / 9thSC (A))
    - United States Army Intelligence and Security Command, sotto il controllo operativo del ARCYBER per le azioni cyber-correlate.
        - 1 ° Information Operations Command (Esercito)
        - 780 Military Intelligence Brigade (Cyber)
- Fleet Cyber Command / Decima Flotta Navale
    - Naval Network Warfare Command
    - Navy Cyber Defense Command Operations
    - Comandi operativi Informazioni navali
    - Combined Task Forces
- Air Forces Cyber / Ventiquattresima Air Force (Aviazione)
    - 67th Cyberspazio Operations Wing
    - 688 Cyberspazio Operations Wing
    - 624 Operations Center
    - 5 ° Combat Communications Group
- Marine Corps Cyberspace Command (Marines)

DOMANDA 4)

La NSA negli ultimi anni ha dichiarato guerra aperta alla cyber war. La NATO ultimamente ha inserito gli atti di cyberwar, cioè le aggressioni ad una nazione tramite attacchi informatici, come riconducibili ad atti di guerra in conformità all’articolo 5 del Trattato Nord Atlantico. Secondo le

stime fatte dal Center for Strategic and International Studies di Washington la cyber war fa girare tanti soldi quanti riesce a metterne in circolo il traffico internazionale di droga. Secondo i dati dello studio americano l'Italia, a causa degli attacchi hacker, ha subito perdite per 875 milioni di dollari l'anno. Gli Stati Uniti, la Germania e la Cina da soli sono stati sottoposti a incursioni da parte di hacker per un valore complessivo di 200 miliardi di dollari nel 2013. Gran parte degli attacchi informatici sono dovuti al furto di proprietà intellettuali e allo spionaggio economico attuato dagli stessi governi. La Cina, ad esempio, è stata accusata dagli Stati Uniti di essere uno dei principali "ladri" di informazioni e brevetti ai danni delle imprese Usa. Anche le infrastrutture degli Stati Uniti sono costantemente sotto attacco informatico, anche da parte di paesi come la Cina che ha un fortissimo esercito di cybersoldati e che lavorano per creare disservizi, e perdita di informazioni. La logica del terrorismo applicata al cyberspace potrebbe produrre scenari catastrofici: virus informatici potrebbero neutralizzare i sistemi di difesa di una nazione, mandare in tilt acquedotti e sistemi elettrici. Gli Usa nel ruolo di superpotenza continua a muoversi in direzione di una proiezione del potere militare nello spazio cibernetico, definito come 'nuovo teatro di operazioni' dalla National Security Strategy elaborata dal Dipartimento della Difesa già nel 2005. Il dominio del cyberspace consentirà una gestione del potere che, intervenendo con azioni di disturbo (jamming) e attacchi mirati, potrebbe risparmiare molte vite di militari. Nel giugno 2014, il Pentagono ha nominato l'ammiraglio di squadra navale **Michael Rogers** comandante della cyber security della Us Navy, a capo della National Security Agency ed al comando delle unità contro i cyber attacchi. Rogers, esperto di codici, sostituisce il generale di squadra aerea **Keith Alexander** e costituisce la prima mossa del presidente **Barack Obama** per il nuovo corso della NSA coinvolta nelle critiche per il caso **Datagate**, scatenato dalle rivelazioni dell'ex analista **Edward Snowden.**

DOMANDA 6)

Il Centro di Cooperazione Cyber Defence NATO di eccellenza (Estonian : *K5* o *NATO küberkaitsekoostöö keskus)* è uno dei Centri di Eccellenza della NATO e si trova a Tallinn , Estonia . Il Centro è stato creato il 14 maggio 2008, ha ricevuto pieno riconoscimento da parte della NATO e ha raggiunto lo status di organizzazione militare internazionale il 28 ottobre 2008. Il Centro svolge attività di ricerca e formazione in materia di sicurezza informatica e comprende uno staff di circa 40 persone. Il Centro di Tallinn è uno dei 18 accreditati (COE), per la formazione su aspetti delle operazioni della NATO ad alto livello tecnico. E' finanziato a livello nazionale e multi-nazionale.

Compito della struttura è quello di:

- migliorare l'inter-operabilità della difesa contro attacchi cibernetici all'interno del Network Enabled Capability NATO (NNEC),
- migliorare la sicurezza delle informazioni e potenziare l'educazione ad una cultura della difesa cibernetica,
- fornire il supporto per la sperimentazione (anche on-site),
- analizzare gli aspetti legali della difesa informatica.

Il centro ha anche altri compiti:

- contribuire allo sviluppo delle politiche di sicurezza della NATO in materia di cyber-difesa e la definizione del campo di applicazione,
- realizzazione di progetti di formazione, campagne di sensibilizzazione, workshop e corsi.

DOMANDA 7)

Si. Siamo in piena cyber war che rischia di mandare in frantumi la privacy di persone, società e nazioni. Il cyber terrorismo rappresenta una sfida alla stabilità, alla prosperità e alla sicurezza di tutte le nazioni, e le azioni di attacco possono essere originate da entità statali, da terroristi, da gruppi criminali o da individui dediti alla ricerca d'informazioni o alla distruzione e al danneggiamento dei sistemi informatici e dei dati in essi contenuti. La Nato, nel prossimo decennio, ha intenzione di assumere sempre più un ruolo di difesa collettiva perché le sfide del futuro sono sempre più la cyber war e gli attentati alla libertà di navigazione sul web.

----- Original Message -----
From: Pierluigi Mele
To: mavil
Sent: Wednesday, January 21, 2015 6:05 PM
Subject: Domande per Intervista Rainews24

Ciao Antonella, ecco le domande sulla Cyberwar. Pierluigi