La dimensione tecnologica nel terrorismo islamico

Antonella Colonna Vilasi[*] Luca Nicotra[**]

Sunto: *Intervista ad Antonella Colonna Vilasi sul ruolo che gioca l'informatica sia nelle strategie delle azioni terroristiche dell'ISIS, e più in generale nella cosiddetta "guerra cibernetica" (cyberwar), sia nelle attività dell'Intelligence volte a contrastare queste azioni.*

Parole Chiave: Guerra cibernetica, cyberspazio, intelligence, ISIS

Abstract: *Interview with Antonella Vilasi Colonna on the role that information technology plays in both strategies of terrorist actions of ISIS, and more generally in the so-called "cyber war" (cyberwar), both in Intelligence activities against these actions.*

Keyword: Cyberwar, cyberspace, intelligence, ISIS

Citazione: Vilasi Colonna A., Nicotra L., *La dimensione tecnologica nel terrorismo islamico*, «ArteScienza», Anno II, N. 3, pp. 75-84.

Per la nostra Rivista, che si occupa di aspetti interdisciplinari, può essere interessante capire il ruolo che gioca l'informatica sia nelle strategie delle azioni terroristiche dell'ISIS, e più in generale nella cosiddetta "guerra cibernetica" (cyberwar), sia nelle attività dell'Intelligence volte a contrastare queste azioni. A tal proposito ho rivolto alcune domande alla professoressa Antonella Colonna Vilasi, massima esperta italiana femminile e autrice di numerose pubblicazioni sull'Intelligence.

Luca Nicotra

[*] Presidente del Centro Studi sull'Intelligence "UNI". Insegna Intelligence in numerose agenzie e università; mavil@tiscali.it.

[**] Ingegnere e giornalista. Presidente dell'Associazione culturale "Arte e Scienza" e direttore responsabile del periodico «ArteScienza»; luca.nicotra@fastwebnet.it.

D - Cara Antonella, vorrei rivolgerti alcune domande sul ruolo che secondo te l'Intelligence può svolgere per contrastare le azioni terroristiche dell'ISIS in Occidente, con particolare riguardo all'uso delle tecnologie informatiche. La presenza, nello scenario mondiale, del sedicente Stato Islamico ISIS costituisce una minaccia per tutti gli stati democratici che preoccupa non soltanto le Istituzioni ma anche le singole persone, per l'inaudita ferocia delle sue azioni. Una minaccia ancora più inquietante per l'Occidente, perché proveniente da un vero e proprio "esercito invisibile" che presenta caratteristiche che trascendono quelle del terrorismo tradizionale di stampo politico cui eravamo abituati nel passato. Molti *foreign fighter* che alimentano le fila di questo esercito provengono da Paesi europei e quindi possono disporre di appoggi naturali nei loro stessi Paesi d'origine per poter organizzare azioni terroristiche. Inoltre spesso si tratta di persone che hanno una eccellente conoscenza degli strumenti informatici, che usano, come purtroppo tutti sanno, per azioni sia di propaganda e diffusione delle loro azioni terroristiche sia di reclutamento.

R - Come hai detto tu stesso, molti affiliati del Califfato sono giovani cresciuti in Occidente e che hanno studiato in università europee. Non è quindi escluso che abbiano la capacità di portare avanti operazioni di guerra cibernetica. 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 e i suoi fiancheggiatori, capaci di inserirsi persino in uno dei sistemi più protetti del mondo. Questa dimensione totale del conflitto sarebbe stata impensabile e ingestibile per un gruppo terroristico fino a qualche anno fa. L'ISIS però ha fatto un salto di qualità notevole. Infatti, 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), con frasi e video inneggianti al Califfato. È la prima volta che una formazione jihadista utilizza

tattiche di guerra cibernetica (*cyberwar*) contro account legati a uno stato. Se l'ISIS possiede una squadra specializzata di hacker, la sua connotazione di gruppo jihadista supera e deborda la sua originaria identità e assume quella di "esercito". Questo attacco cibernetico è stato sferrato dall' ISIS pochi giorni dopo la strage di Charlie Hebdo, 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.

D - Certamente hanno voluto dar prova delle loro potenziali capacità di *cyberwar*. In queste incursioni mediatiche nei siti di istituzioni pubbliche e private, però, non potrebbero esserci dei falsi proseliti che si spacciano per seguaci dell'ISIS ma non lo sono?

R - È possibile. 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». In effetti, alcuni esperti ritengono che si tratti di gruppi che affermino di agire nel nome del jihad ma non siano assolutamente collegati con lo Stato Islamico.

D - Per molti anni ho lavorato nell'industria della difesa, nel campo della guerra elettronica, che può essere definita come l'utilizzo a fini bellici delle onde elettromagnetiche. La società romana nella quale lavoravo era leader mondiale nel campo delle contromisure elettroniche, complessi sistemi hardware e software in grado di manipolare le onde elettromagnetiche per neutralizzare alcune azioni offensive del nemico. Una tipica contromisura elettronica è quella che consente di deviare dal bersaglio un missile a guida infrarossa, che in assenza di tale contromisura elettronica colpirebbe senza possibilità di scampo un aereo a reazione, perché sarebbe guidato dalle radiazioni infrarosse del gas di scarico

dell'aereo stesso. Un analogo utilizzo "bellico" esiste nel campo dell'informazione manipolata dagli strumenti informatici?

R - Certamente. Come ho già detto prima si chiama "guerra cibernetica" o con termine anglosassone *cyberwar*, caratterizzata per l'uso, a fini bellici o di intelligence o di spionaggio industriale, delle tecnologie informatiche e dei sistemi di telecomunicazione che le impiegano. 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.

D - Il ricorso alla guerra cibernetica sta divenendo sempre più massiccio. Quali sono le sue caratteristiche?

R - Gli attacchi informatici contro gli stati 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 .

Per esempio, il *Worm Stuxnet* è stato un attacco informatico agli impianti nucleari iraniani, attuato nel 2010 da Israele e Stati Uniti per danneggiare le centrifughe nucleari iraniane.

D - Gli Stati Uniti d'America, che sono il Paese più avanzato nel campo informatico, come si sono organizzati per contrastare gli attacchi cibernetici?

R - È stato istituito il *Cyber Command* (USCYBERCOM), un comando delle forze armate americane subordinato al Comando Strategico degli Stati Uniti. 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 militari di difesa. Il *Cyber Command* è composto da diverse strutture:

- 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 dell' ARCYBER per le azioni cyber-correlate.
  - 1 ° Information Operations Command (esercito)
  - 780 Military Intelligence Brigade (Cyber)

- Fleet Cyber Command (Decima Flotta Navale, marina militare)
  - Naval Network Warfare Command
  - Navy Cyber Defense Command Operations
  - Comandi operativi Informazioni navali
  - Combined Task Forces
  - Air Forces Cyber (Ventiquattresima Air Force, aviazione militare)
  - 67th Cyberspazio Operations Wing
  - 688 Cyberspazio Operations Wing
  - 624 Operations Center
  - 5 ° Combat Communications Group

- Marine Corps Cyberspace Command (marines)

D - Per quali ragioni alcuni Paesi dedicano molte risorse alla guerra cibernetica e quali sono i tipi di danni che può procurare?

R - Secondo le stime fatte dal *Center for Strategic and International Studies* di Washington la *cyberwar* 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, sopratutto da parte della Cina, che ha un fortissimo esercito di cybersoldati che lavorano per creare disservizi e perdita di informazioni.

La National Security Agency (NSA) negli ultimi anni ha dichiarato guerra aperta alla *cyberwar*. 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.

D - Però gli stessi USA, come tu stessa hai ricordato a proposito degli attacchi informatici alle centrali nucleari iraniane, hanno utilizzato la guerra cibernetica. È poi ancora nella memoria di tutti il *Datagate*, la gigantesca operazione di monitoraggio di massa fatta proprio dalla NSA e dal GCHQ britannico in collaborazione con le altre tre potenti agenzie segrete di Australia, Canada e Nuova Zelanda, verso tutti i Paesi europei e i loro governi, con forti rimostranze da parte di molti leader politici europei.

Certamente, ancora più inquietante è la prospettiva di un utilizzo della *cyberwar* da parte di gruppi terroristici, l'ISIS in primo piano.

R - La logica del terrorismo applicata al cyber spazio 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 cyber spazio 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 e 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.

D - La guerra cibernetica delinea un quadro poco rassicurante a livello mondiale. Lo stesso Edward Snowden ha recentemente affermato il 17 aprile scorso, intervenendo dalla Russia al IX Festival Internazionale del Giornalismo a Perugia: «Proprio perché c'è il rischio terroristico e le persone sono sempre più consapevoli delle opportunità di crittografare le proprie comunicazioni, i governi pretendono sempre più le chiavi di quelle trasmissioni e di quei contenuti addirittura senza doverle decifrare. Spingono per ottenere delle 'backdoor' da cui entrare per sottrarre informazioni ma dalle quali, questo il rischio sottovalutato, possono far breccia anche altri governi, penso a quello cinese, o gli stessi gruppi terroristici che vorremmo contrastare. Insomma, stiamo creando in tutti i sistemi di comunicazione una vulnerabilità di fondo che costituirà una minaccia perenne».

R - Si. Siamo in piena *cyberwar* 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 *cyberwar* e gli attentati alla libertà di navigazione sul web.

D - Quali sono le strutture organizzative sulle quali la NATO può contare per contrastare attacchi cibernetici verso i suoi stati membri?

R - Il Centro di Cooperazione Cyber Defence NATO di eccellenza (*K5* o *NATO küberkaitsekoostöö keskus)* è uno dei Centri di Eccellenza della NATO e si trova a Tallinn, capitale dell'Estonia . È stato creato il 14 maggio 2008 e ha ricevuto pieno riconoscimento da parte della NATO ottenendo 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. È 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 a 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.