L'INTERVISTA / ALAIN VUITEL / capoprogetto Comando ciber dell'esercito

«Anche lo spazio cibernetico è diventato terreno di battaglia»

Moreno Bernasconi

Il divisionario Alain Vuitel, 59 anni, è capoprogetto del Comando ciber dell'esercito. Questo organo, che dovrebbe diventare operativo il 1. gennaio del 2024, avrà il compito di proteggere i sistemi informatici dai ciberattacchi e far sì che l'esercito possa intervenire anche nello spazio elettromagnetico e nel ciberspazio. Giovedì 2 novembre, alle 18, al Lac di Lugano,il divisionario Vuitel prenderà parte, con la «ministra» della Difesa Viola Amherd, a un incontro organizzato dall'Associazione per la Rivista Militare Svizzera di lingua italiana. Lo abbiamo intervistato.

Alain Vuitel: «La formazione e l'impiego di specialisti di milizia è un vantaggio per tutti». © KEYSTONE/ANTHONY ANEX

Signor Vuitel, la macchina della Confederazione è pesante e la tentazione di moltiplicare gli uffici federali aumenta la burocrazia. Perché creare un nuovo Comando cibernetico?
«Non viene creato un ufficio federale supplementare all'interno del Dipartimento federale della difesa. Semplicemente, l'attuale Base di aiuto alla condotta (BAC) cesserà di esistere e lascerà il posto al Comando cibernetico, che avrà lo statuto di Ufficio federale. La creazione di questo comando è una risposta alla crescita esponenziale delle minacce provenienti dallo spazio cibernetico e elettromagnetico dovute in particolare agli sviluppi tecnologici in continua accelerazione. Lo spazio cibernetico è ormai diventato un nuovo campo d'azione e di conflitto, sia da parte di privati sia da parte degli Stati. Come dimostra ad esempio la guerra in Ucraina, lo spazio cibernetico è diventato un terreno di battaglia di cui non si può non tener conto. Lo è e lo era già prima dello scoppio delle ostilità militari classiche».

Quale sarà il campo d'azione del nuovo Ufficio federale, i suoi compiti e il suo funzionamento?
«Il Comando ciber ha per compito la protezione, il trattamento e la messa a disposizione di tutti i dati critici informatici per l'impiego del nostro esercito e dei suoi partner in seno alla rete nazionale della sicurezza. Esso permette così la realizzazione di tutte le azioni dell'esercito (aeree e di terra), creando le condizioni necessarie per mettere a disposizione di chi prende decisioni - dai vertici ai livelli più bassi - le informazioni necessarie per realizzare con successo le proprie missioni. Grazie ai vantaggi che offre il trattamento dei dati e la loro messa a disposizione, essi avranno un vantaggio in termini di sapere e di decisione che permetterà loro di adottare i mezzi più adeguati, nel momento più opportuno e nel posto più opportuno. Mi permetta una similitudine: il Comando cibernetico può essere considerato il sistema nervoso del nostro esercito. Assicura infatti la connessione fra i suoi organi sensoriali e le sue membra (truppe e altri sistemi d'arma) assicurando nel contempo il trattamento dei dati raccolti, trasformandoli in informazioni utilizzabili per i decisori militari (Stati maggiori e Comandanti). Il funzionamento di questo sistema nervoso centrale sempre attivo è essenziale per assicurare non solo il funzionamento ma ancor di più il successo di un esercito e delle sue componenti. Proprio per la sua funzione essenziale per l'insieme del sistema, è assolutamente necessario che sia sottoposto ad un alto grado di protezione, da subito. Il Comando cibernetico è quindi la prima linea di difesa del nostro esercito».

Il comando cibernetico è la prima linea di difesa del nostro esercito

L'obiettivo è permettere al nostro esercito di pianificare e realizzare operazioni in modo autonomo

La cibersicurezza del nuovo aereo da combattimento F-35A è garantita molto bene

Quanto costerà? Il suo finanziamento è compreso nel budget annuale dell'esercito?
«Il Consiglio federale ha definito lo scorso anno i bisogni a cui risponde il comando cibernetico per assicurare lo sviluppo futuro delle capacità del nostro esercito. Nel corso dei prossimi 10-15 anni verranno investiti circa 2,5 miliardi di franchi. Il finanziamento si farà nell'ambito del budget annuale dell'esercito votato dal Parlamento».

Chi ci lavorerà? Funzionari, professionisti dell'esercito o anche militari di milizia?
«Dal mese di gennaio prossimo, il Comando cibernetico potrà contare su circa 700 collaboratori, funzionari civili e militi di carriera. La Brigata di aiuto al comando 41, vi rappresenta la componente di milizia. Forte di 12.000 militi, gioca un ruolo chiave: senza l'impegno della nostra milizia il Comando ciber non potrebbe assicurare le sue prestazioni di condotta integrata a profitto del nostro esercito e dei suoi partner in seno alla rete nazionale di sicurezza».

Quando si entra nel campo dei big data ci vogliono strumenti di gestione e di salvaguardia di dati molto sofisticati e potenti. Lavorate anche con centri di ricerca e i calcolatori degli Istituti svizzeri, come ad esempio il Centro di calcolo del Poli di Zurigo?
«Nel settore dei big data collaboriamo strettamente con Armasuisse Science et Technologie. Questo organo dispone di un Cyber Defence Campus basato alla Scuola politecnica federale di Losanna, con una antenna presso il Poli di Zurigo. Questa collaborazione è estremamente importante: per ragioni di risorse il Comando ciber non può sviluppare tutto in proprio. Dipendiamo dalle competenze di altri istituti di alta specializzazione. Ciò permette di sfruttare sinergie che offrono un grande valore aggiunto. E ciò che è ancora più importante è il nostro sistema di milizia. Nel campo cibernetico ed elettromagnetico la formazione e l'impiego per i nostri scopi degli specialisti di milizia rappresenta una situazione vincente per tutti. Grazie ad un curricolo di formazione da noi offerto, formiamo specialisti preparati per la difesa del nostro Paese nel terzo millennio. Così facendo, contribuiamo attivamente alla lotta contro la penuria di personale qualificato nei settori della cibernetica e l'informatica. E diamo ai nostri militi la possibilità di esercitare professioni attrattive rivolte al futuro. Grazie alla creazione del programma SPARC (programma di formazione gratuito) coinvolgiamo giovani a partire dai 16 anni che si interessano alla cibersicurezza e all'informatica».

In tempi di altre minacce, i fortini servivano a proteggere le infrastrutture vitali, armi di difesa e risorse alimentari. Oggi, nell'era digitale e di fronte a nuove minacce, come proteggiamo informazioni vitali per preservare il nostro Paese?
«Il Comando cibernetico costruisce proprio a questo fine una nuova piattaforma numerica. Suo scopo è di permettere al nostro esercito di pianificare e realizzare in futuro operazioni in modo autonomo, ininterrottamente, e in tutti i campi di azione federando le informazioni necessarie per realizzare questo obiettivo. Questa piattaforma standardizzata è quindi orientata risolutamente all'impiego dell'esercito e dei suoi partner nella rete nazionale di sicurezza. Concretamente, la piattaforma sarà costituita di diversi centri di calcolo connessi fra loro tramite una rete di condotta a maglie molto strette ed estesa all'insieme del territorio nazionale. Questa infrastruttura robusta, sicura e resiliente comprenderà un gran numero di dispositivi realizzati per resistere alle condizioni più estreme».

Siamo un Paese neutrale, non membro dell'UE e tantomeno dell'Alleanza militare atlantica. Come faremo ad essere autonomi nel campo della difesa informatica? È possibile?
«Il nostro obiettivo è di assicurarci uno sfruttamento completamente autonomo della nostra nuova piattaforma numerica. Il suo sviluppo dipende tuttavia da diverse collaborazioni. La Svizzera e il suo esercito non dispongono in effetti delle risorse tecniche e della perizia necessari a questo fine. Ricorrere a competenze esterne significa per noi disporre delle migliori soluzioni per poter rispondere ai nostri bisogni. L'utilizzazione conseguente degli standard esistenti in questo campo rappresenta anche per noi una condizione necessaria».

Viviamo un'epoca di ridefinizione degli equilibri geopolitici e di nuovi conflitti asimmetrici su scala mondiale. Per preservare la neutralità elvetica, garantirci un'autonomia è certo un obiettivo, ma nei fatti dobbiamo scegliere da che parte stare.
«La trasformazione di cui lei parla si accompagna sul piano tecnologico da una vera rivoluzione digitale delle nostre società. Un'evoluzione che ha prodotto un aumento massiccio della produttività del lavoro e del nostro benessere. Parallelamente, essa ha evidenziato nuove vulnerabilità. In un tale contesto in costante trasformazione bisogna poter disporre di una ampia rete di contatti internazionali per stare al passo con gli sviluppi sempre più rapidi e prendere coscienza dei rischi e dei pericoli che tutto ciò comporta. Nell'ambito di un programma di collaborazione politicamente legittimato, il nostro esercito si associa nel campo cibernetico a diverse attività in corso. Segnatamente a diverse esercitazioni, d'intesa con i Paesi a noi vicini e rispettivamente nel quadro della NATO. Ciò ci permette di accrescere le nostre competenze essenziali per rafforzare la nostra capacità di difesa nel campo cibernetico ed elettromagnetico».

Abbiamo acquistato gli F-35A americani. Macchine da guerra ma anche formidabili macchine di elaborazione e trasmissione di dati. Saremo quindi sempre sotto controllo americano... e magari manipolati in caso di ingaggio della NATO in un conflitto armato ai confini dell'Europa?
«La Svizzera aspira a una autonomia il più grande possibile. Un'indipendenza totale dal produttore e dal Paese di fabbricazione non è possibile. La cibersicurezza dell' F-35A è garantita molto bene poiché lo sfruttamento del sistema, la sua architettura informatica e le diverse misure di protezione ciber sono parte integrante del concetto globale di questo aereo. La Svizzera decide autonomamente quali dati scambia con altre forze aeree tramite collegamenti di dati o dati logistici trasmessi al fabbricante. Inoltre lo sfruttamento e la manutenzione dell'aereo in Svizzera sono assicurati dalle forze aeree elvetiche e RUAG Svizzera. L'F-35A è usato da numerosi altri Paesi, segnatamente europei, ciò che riduce la dipendenza di un singolo Paese come la Svizzera. Segnalo inoltre che la tecnologia dei sistemi che permettono l'interoperabilità è anch'essa statunitense, compresa quella per i modelli di costruttori europei (ad esempio Datalink, navigazione satellitare)».

Vorrei concludere con una domanda di attualità, ad uno specialista come lei. Come è possibile che Israele, che dispone di servizi segreti formidabili, non abbia visto venire i brutali attacchi convenzionali di Hamas?
«Il ciber non è un'arma assoluta, bensì un nuovo campo d'azione delle forze armate, accanto a quelle tradizionali di terra, di mare e aerei, e sempre più spaziali. È troppo presto per fare un primo bilancio di questa guerra brutale e in particolare dell'operato dei servizi di intelligence. Vorrei tuttavia sottolineare qui che pensare di prevedere tutto è un'illusione. Una minaccia risulta dal prodotto fra il potenziale di un attore e le sue intenzioni. È più facile identificare il potenziale che le vere intenzioni. Giacché queste ultime possono effettivamente modificarsi in tempi brevissimi».