

Verso il comando cibernetico

L'essenza è ciò che è la luce del sole / proprio come la luce della luna. / Entrambe hanno luce, hanno forma / entrambe hanno oscurità e ritardi. / Non si concepisce l'oscurità / finché non s'è in ritardo con la luce. (Jack Kerouac)

Cosa deve fare dunque l'esercito svizzero per difendersi dagli attacchi informatici e dalla disinformazione? Lo ha spiegato il divisionario Alain Vuitel invitato come ospite d'onore all'ARMSI e presentato

al LAC dal presidente Marco Netzer. Alain Vuitel sarà infatti dal gennaio prossimo il capoprogetto del comando Cyber dell'esercito elvetico; avrà il compito di proteggere i sistemi informatici dai cyberattacchi intervenendo nello spazio elettromagnetico con la forza necessaria e la capacità di agire per difendere la Svizzera 365 giorni all'anno, 24 ore su 24. Oggi non c'è una piattaforma unica a servizio dell'esercito, ma si è tributari di 35 diversi centri di calcolo, ognuno con le sue specifiche regole e particolarità. Il che significa oltretutto un tributo costoso e artificioso. Così si è optato per una nuova piattaforma che si basa su tre centri di calcolo, di cui due protetti internamente e uno a disposizione delle truppe e dei centri locali, in modo da assicurare rapidità di esecuzione e decisione. In tal modo anche i caccia F35 avranno a disposizione i dati necessari per il loro miglior funzionamento. La creazione del comando è una risposta alla crescente necessità di una difesa



Alain Vuitel, capoprogetto del comando Cyber dell'esercito, e Marco Netzer, Presidente dell'ARMSI.

puntuale e decisiva dagli attacchi informatici. Tutto dipende dalla connettività, bisogna eliminare gli ostacoli prima che questi paralizzino il proprio apparato. Cosa vogliamo con questo comando? Rafforzare prima di tutto la capacità di difesa e la sicurezza con una nuova piattaforma e ciò avviene grazie all'expertise dei collaboratori. In tal modo possiamo garantire la sicurezza infrastrutturale e informatica utilizzando al meglio il digitale a vantaggio dei decisori quali gli Stati maggiori e i comandanti. Ci assicuriamo in tal modo una libertà di manovra per intervenire nel sistema, utilizzando anche le reti esterne e l'interconnessione per il necessario e opportuno scambio di informazioni. La base resta comunque il personale interno, in grado di garantire protezione e intelligenza assistita dai dati. Per questo motivo e ulteriore sicurezza, ogni dipendente non avrà a disposizione tutta la trafila decisionale e nessuno avrà il controllo completo, ma funzionerà a scomparti, anche

perché – al di là della professionalità tecnica – la cosa decisiva resta la capacità di lavorare in team. Dal prossimo gennaio il Comando cibernetico potrà contare su circa 700 collaboratori, funzionari civili e militari esperti d'informatica provenienti dal mondo accademico e industriale. Dipendiamo infatti dalle competenze di altri istituti come il Politecnico federale di Losanna o Zurigo, con la creazione del programma gratuito SPARC, coinvolgendo giovani a partire da 16 anni interessati alla sicurezza informatica e cibernetica. La scuola di reclutamento per la selezione occupa un arco temporale di circa sei settimane e la formazione continua è essenziale per innalzare il livello di professionalità. Il nostro approccio è basato sui dati e questa resta la prima linea di difesa. Quanto all'Intelligenza Artificiale essa funziona con dati e parole chiave, ma non è autonoma, bensì trattasi di intelligenza assistita per rafforzare la capacità di difesa. (CBP)