Zeitschrift: Rivista Militare Svizzera di lingua italiana : RMSI
Herausgeber: Associazione Rivista Militare Svizzera di lingua italiana
Band: 95 (2023)
Heft: 6

Artikel: Verso il Commando Cyber : una lunghezza d'anticipo
Autor: Annovazzi, Mattia
DOI: https://doi.org/10.5169/seals-1050291

Verso il Comando Ciber – Una lunghezza d'anticipo

Associazione per la ARMSI
Rivista Militare Svizzera di lingua italiana

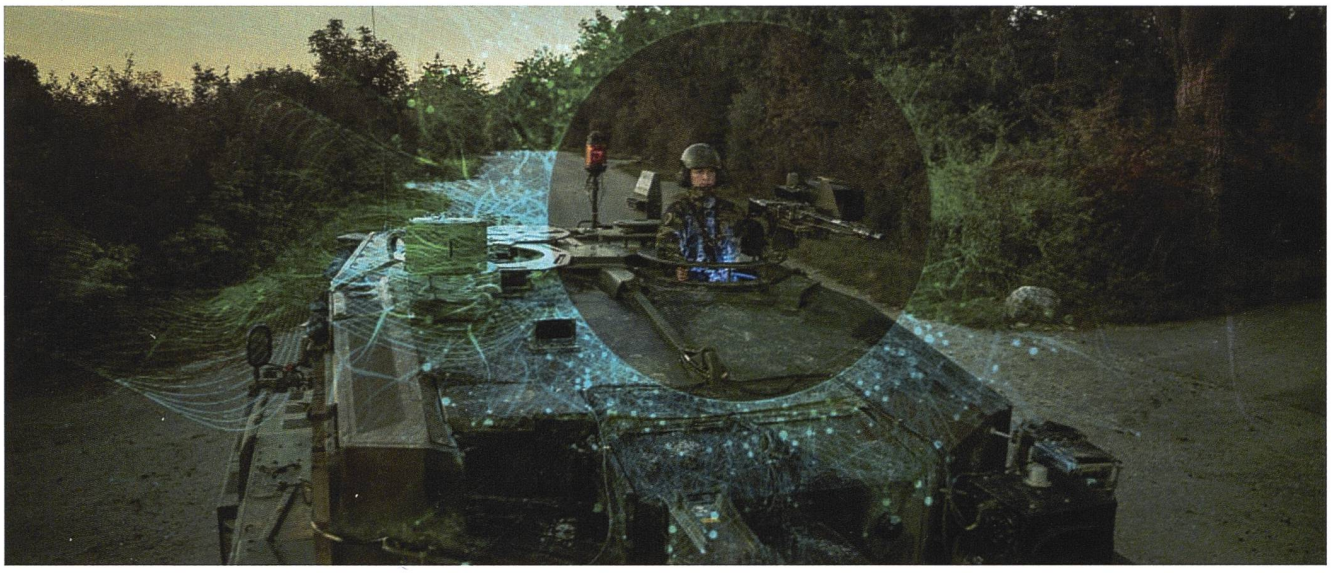
La seconda parte della Conferenza 2023 dell'ARMSI ha proposto un tema di stretta attualità.

colonnello Mattia Annovazzi

La Base d'aiuto alla condotta (BAC) dell'esercito è stata sciolta con effetto al 31 dicembre 2023. Si conclude così un'era quasi ventennale. Questa data segna anche il passaggio di consegne al nuovo Comando Ciber.

La BAC trae le sue radici dall'Ufficio federale dell'aiuto alla condotta, a sua volta nato all'inizio del nuovo millennio dal raggruppamento della Divisione principale informatica del DMF e di alcune parti del Gruppo dell'aiuto alla condotta. All'epoca l'attività era concentrata sulla fornitura di prestazioni con mezzi informatici civili su reti parzialmente militari. Tale evoluzione si è conclusa con la riforma Esercito XXI. Come primo capo della BAC, il divisionario KURT NYDEGGER aveva assunto la responsabilità di oltre 700 collaboratori.

Nel 2004 è stata portata a termine la riorganizzazione dell'informatica della Confederazione battezzata "NOVE-IT". Una delle conseguenze di questa riorganizzazione è stata l'uniformazione dei processi nel campo dell'informatica. Negli anni successivi la BAC si è evoluta a fornitrice di prestazioni TIC primaria per l'intero DDPS, nonché per altri dipartimenti e organi federali. La sua attività abbracciava i sistemi informatici dell'Amministrazione federale e i sistemi militari, come ad esempio il sistema d'informazione e di condotta delle Forze terrestri (FIS FT).
Nel corso degli anni sono stati fatti molti progressi tecnologici nel settore TIC e sistemi di condotta, e parallelamente è pure aumentata la loro complessità. Le esigenze nei confronti della BAC continuavano ad aumentare in conseguenza al crescente numero di progetti e sistemi per la creazione e la susseguente gestione delle strutture imposte dall'evoluzione tecnologica e dalla digitalizzazione e tutto questo con risorse pressoché invariate. Pure la protezione delle infrastrutture contro le minacce ciber acquistava sempre maggiore importanza e di pari passo si faceva anche sempre più impegnativa per effetto della crescente interdipendenza tra sistemi civili e militari.
Nel 2016 l'allora capo del DDPS, Guy Parmelin, prese la decisione di separare l'informatica civile da quella militare. Questo è stato il primo passo verso lo scorporo TIC tuttora in atto nel DDPS così come nell'Aggruppamento Difesa. Lo scorporo concerne sia la burotica BURAUT sia le applicazioni specialistiche. L'obiettivo è di affidare l'informatica della parte amministrativa a partner civili come l'Ufficio federale dell'informatica e a terzi, mentre i sistemi, le applicazioni e i servizi critici per gli impieghi saranno gestiti dal Comando Ciber.



VICTORINOX

RESCUE TOOL

PROGETTATI DAI PROFESSIONISTI, PER I PROFESSIONISTI

Dal taglia cinture di sicurezza al rompivetro e al seghetto per il taglio di vetri infrangibili. Quando ogni secondo conta, puoi affidarti a Rescue Tool.

FROM THE MAKERS OF THE ORIGINAL SWISS ARMY KNIFE™
ESTABLISHED 1884

Per maggiori informazioni
www.victorinox.com

Il divisionario ALAN VUITTEL, capo progetto Cdo Ciber fino al dicembre 2023 (capo dello stato maggiore dell'istruzione operativa dal gennaio 2024), ha presentato le ultime novità e le sfide future del Cdo Ci.

Quanto al contesto attuale ha sottolineato il fatto che ci troviamo in uno stato di mutamento permanente e multicrisi: covid, guerra in Ucraina e in medio oriente, approvvigionamento energetico, inflazione, riarmo, fame nel mondo, crisi climatica, crisi migratoria. Elementi con rilevanza sistemica, che generano criticità a livello sociale e per l'impiego. Il mondo sta diventando meno globale, meno influenzato dalla civiltà occidentale, meno democratico, più frammentato e pericoloso, ed è caratterizzato da volatilità. Come militare ha affermato di essere preoccupato per la situazione e per i pericoli che potrebbero derivare da un cattivo apprezzamento della situazione, con rischio elevato di errori o incidenti derivanti da una logica di escalation. "Un antico adagio africano dice che quando gli elefanti lottano è l'erba che soffre". Occorre prendere a cuore la nostra difesa e la nostra capacità di affrontare la situazione.

"Nel nostro mondo vi è poi un aspetto che è rivoluzionario: la digitalizzazione che ci accompagna permanentemente a partire dai nostri telefoni cellulari. Un mondo creato interamente dall'essere umano che non esiste ma che è sempre più critico per gli individui e la loro vita. L'importanza della connettività è tale che diviene per l'Esercito la prima linea di difesa". Dall'esistenza e dal funzionamento del mondo digitale dipende la nostra capacità di agire e manovrare. La guerra in Ucraina ha mostrato il ruolo chiave di questa dimensione digitale, dal livello strategico al livello tattico. Il presidente ucraino due giorni dopo l'attacco del 24 febbraio 2021 si trovava con i suoi consiglieri, registra un video e dice tre cose: sono qui, siamo qui, e restiamo qui. La forza di questo messaggio, oltre alle parole è data dal fatto che il suo computer portatile fosse connesso in rete e quindi il suo messaggio venisse moltiplicato nel mondo. Il sostegno all'Ucraina dipende da questa connettività e il fatto di essere presenti sulle reti di informazione. Ma anche a livello tattico è molto importante: "in guerra c'è una regola purtroppo dimenticata che consiste nel fatto che occorre eliminare il nostro avversario prima che lo faccia lui". L'importanza di disporre dell'informazione al momento giusto ha un ruolo cruciale sulla capacità di adempiere le missioni e di sopravvivere. Si parla di *"rete integrata sensori – servizio informazioni – condotta – effetti" (Sensor-, Nachrichten-, Führungs- und Wirkungsverbund, SNFW)* oppure di *OODA loop* (Observe, Orient, Decide, Act; v. già RMSI 04/2019 pag. 32 segg.), allo scopo di poter impiegare i giusti mezzi nel momento giusto. Importante disporre dei dati e che circolino rapidamente.

> " (...) by depriving forces of connectivity, it drives armies back to the 20th century" – Major General Charles Collins, *Mobilising the British Army,* in: The British Army Review, Spring 2023, pag. 8

In Ucraina si assiste al primo conflitto dell'era numerica e in questo campo l'Ucraina dispone di un vantaggio, che dipende anche dall'appoggio del popolo ucraino, delle potenze occidentali e – questa è anche una rivoluzione – dei grandi gruppi in campo IT, come Microsoft (ma anche altri), impiegata molto nella protezione delle reti ucraine. Un esercito privo di connessioni ritorna al livello del XIX secolo (con corrieri e carta) e non ha alcuna possibilità contro un esercito digitalizzato. Anche i migliori sensori, senza la *connettività* che trasporti l'informazione, non serviranno a niente. Va rilevata l'importanza della difesa aerea nei confronti della minaccia di droni, missili, missili da crociera. La difesa aerea dipende da un livello molto elevato di connettività per poter agire rapidamente contro obiettivi che si muovono velocemente nella terza dimensione. Se si tratta di riguadagnare terreno o di condurre una manovra offensiva, la connettività serve per coordinare la manovra e il fuoco. La condotta avviene in rete, per connettere i sensori e i mezzi di esplorazione, consolidare dati e informazioni in una rappresentazione/immagine della situazione, quindi prendere decisioni e condurre la manovra.

Dalla fine del 2020, nel quadro della visione per rinforzare la nostra capacità di difesa, una linea direttrice è rappresentata dall'importanza del numerico (ndr. v. comunque quanto fatto già a suo tempo dal precedente capo dell'Esercito, cdt C PHILIPPE REBORD, in merito al programma FITANIA concernente l'infrastruttura di condotta, tecnologia dell'informazione e collegamento con l'infrastruttura di rete dell'Esercito, di cui la RMSI ha riferito ampiamente). Il Cdo Ciber avrà un ruolo fondamentale per l'efficienza digitale. L'Esercito sfrutterà la digitalizzazione in primo luogo per l'impiego rapido e preciso degli effettori. L'intera infrastruttura digitale dovrà essere robusta, resiliente. Dovrà funzionare anche nel caso in cui i sistemi subiscano una certa degradazione e sarà protetta da ciberattacchi. Per sviluppare le capacità, l'Esercito continua nella costruzione di una nuova piattaforma numerica e si dota degli strumenti informatici necessari per operare a livello cibernetico ed elettromagnetico. Nonostante l'ambito sia molto tecnico, sono le persone e l'expertise dei collaboratori che fanno la differenza. Il tutto con lo scopo di avere un vantaggio in termini di conoscenza e decisione.

Il 18 marzo 2022 il Consiglio agli Stati ha votato la modifica della Legge militare prevedendo nell'articolazione dell'Esercito, dal 1° gennaio 2024, il Cdo Ciber. I compiti sono:
(a) garantire la sicurezza dell'infrastruttura TIC rilevante all'impiego (critica);
(b) riuscire ad approfittare dei vantaggi, sfruttando il potenziale della digitalizzazione, mediante la raccolta e il trattamento robusto e sicuro dei dati, collazionandoli in un'immagine comprensibile della situazione (comprensione integrata della situazione) per i

cdt interessati, in modo da generare un vantaggio in termini di conoscenza e decisione;
(c) garantire la libertà di manovra sia nello spazio elettromagnetico sia in quello cibernetico mediante il monitoraggio della situazione 24/7/365 e azioni nello spazio cibernetico ed elettromagnetico [CER], disturbando lo spazio elettromagnetico ed entrando nei sistemi informatici (v. anche RMSI 01/2023 pag. 22).
Nel caso del documento sulla concezione ciber, il Consiglio federale non si è limitato a una presa di conoscenza ma ha dato un mandato di sviluppo di queste capacità. Il relatore ha parlato di una "trilogia" delle concezioni ciber, aerea e terreste: "il nuovo aereo di combattimento potrà dispiegare tutti i suoi effetti (a partire dalla fusione dei dati) solo se disporrà dei dati necessari; quindi occorre uno zoccolo, un sistema nervoso centrale che il Cdo Ciber metterà a disposizione delle forze aeree, ma anche delle forze terrestri".

Occorrono quindi centri di calcolo, reti fisiche o attraverso lo spazio elettromagnetico per permettere una condotta interconnessa a livello organizzativo e tecnico. La realizzazione della nuova piattaforma numerico/digitale è cruciale. Ora si dispone di ben 35 centri calcolo diversi, secondo tecnologie e standard diversi. L'idea è di fare "tabula rasa", attraverso la creazione di 3 centri di calcolo nazionali protetti (due completamente, uno in parte), creandone altri più piccoli per migliorare la ridondanza a livello regionale (ad esempio una base aerea) e in favore della truppa a livello locale. Tutti si baseranno sullo stesso modello e saranno standardizzati in modo da creare una sorta di "cloud", solamente raggiungibile dall'Esercito e dalla Rete integrata svizzera per la sicurezza (RSS). Da tempo la Svizzera è associata a un'iniziativa, la Federated Mission Networking (FMN, standard NATO), con l'idea di poter cooperare con sistemi diversi, con Cantoni e altri attori, anche stranieri, per garantire lo scambio di informazione. Questo sistema potrà funzionare in modalità "degradata"; ovvero i diversi elementi funzioneranno in modo autonomo, anche se non fossero più collegati ai grandi centri di calcolo. L'esercito sarà autonomo nell'utilizzo della nuova piattaforma, mentre nello sviluppo ci si appoggia all'esterno, con un "controllo attento dei punti di entrata, delle dipendenze con l'industria". Il relatore non si è espresso quanto a una possibile collaborazione con la NATO, pur rilevando l'importanza di standardizzare i processi e le piattaforme informatiche, nel caso in cui la politica decidesse di procedere in questo senso. Si tratta di un insegnamento dall'Afghanistan, in cui i partner della coalizione si sono trovati a lavorare con standard differenti.

L'integrazione di altri partner si basa sul principio della sussidiarietà. La prima missione del Cdo Ciber è il funzionamento dell'infrastruttura critica per esercito. L'esercito può poi appoggiare altri partner se i mezzi civili sono esauriti e vi è una decisione politica in proposito.

Per taluni ambiti di nicchia la collaborazione è più stretta, come per prestazioni di crittologia (ad esempio per la polizia, per "decodificare" sistemi informatici). Vi è uno scambio regolare nell'ambito dell'immagine della situazione. "L'idea che un gruppo di ciberspcialisti potrebbero giungere in un'infrastruttura critica non corrisponde alla realtà".

I controlli interni al Cdo Ciber sono svolti dagli organi del Servizio delle attività informative della Confederazione (SIC), sia per i prodotti che riceve, sia per i controlli relativi agli ascolti elettronici; e poi dalla Delegazione delle Commissioni della gestione (DELCDG) del parlamento. A livello di governance è previsto che lo SM dell'esercito controlli sia i dati sensibili, sia il modo in cui viene articolato l'orientamento dell'informatica.

Per quanto riguarda l'acquisizione di personale, il Cdo Ciber propone diverse iniziative.

La *ICT-Warrior* è un'istruzione di base e continua per attirare giovani nei settori IT e ciber. La formazione di un anno permette già l'integrazione in team professionali. Per quanto riguarda la milizia, uno degli insegnamenti della guerra in Ucraina è che si possono istruire rapidamente dei militi a sistemi d'arma perfezionati (come missili anticarro ecc.); ma occorrono anni per istruire uno specialista ciber capace di pianificare e condurre un attacco cibernetico ad esempio a una centrale elettrica o a una rete satellitare e ancora molto più tempo per istruire a respingerlo.

Nel 2022 si è creato il *battaglione ciber 42* e uno *SM specializzato*, in cui emerge la grande forza dell'esercito di milizia, qui composto di ottimi specialisti provenienti dal mondo industriale, economico, accademico, mettendo a frutto il loro *savoir-faire*.

Vi è poi *stage di formazione ciber* (v. RMSI 06/2018 pag. 25 segg.) che si sviluppa su due fasi, la prima di selezione attraverso tutte le scuole reclute della svizzera. Nel quadro della "selezione 1", chi ha interesse può annunciarsi e svolgere un test su un computer, con grado di difficoltà sempre più elevato, così da poter rilevare il potenziale. Nella "selezione 2" vengono valutati 200 candidati, esaminando la loro capacità di lavoro in team e gli aspetti di sicurezza. Su questa base se ne selezionano una ventina, che seguiranno lo stage di formazione, con istruzione base, scuola suff (ndr. la formazione dura 40 settimane, per cui terminano con il grado di sergente). Interessante il servizio pratico, durante il quale i militi svolgono la loro attività presso partner esterni come la polizia, l'industria ecc. Questi militi devono superare un controllo di sicurezza relativo alle persone, di livello 11 o superiore. Il principio in questo campo "zero trust". Inoltre, una persona da sola non ha accesso a tutto un sistema, ma vi è grande compartimentazione per aumentare il livello di sicurezza.

Da citare poi *l'istruzione ciber preparatoria (SPARC)* per attirare giovani talenti dai 16 ai 20 anni sul tema ciber nell'esercito. Permette di aumentare ulteriormente il livello formativo (explorer, poi defender, poi operator) in vista dello stage di formazione ciber, ma anche di un certificato civile riconosciuto. In primavera la giornata d'informazione al Politecnico federale ha attirato 120 giovani.

Queste iniziative sono un "triple-win". L'esercito di milizia approfitta delle conoscenze civili. L'economia approfitta nel contesto della carenza di manodopera di specialisti ciber ben formati. Il cittadino acquisisce un valore aggiunto per la sua carriera professionale e la sua formazione.

> "Victory in combat will depend less on individual capabilities and more on the integrated strengths of a connected network of weapons, sensors and analytic tools" – Generale Goldfein, USA Air Force Chief of Staff, Londra, 18 luglio 2019

In futuro ci si dovrà aspettare un'importante estensione della "logica numerica", con una difesa sempre più orientata a strumenti e dati. Questo approccio incentrato sui dati prevede relazioni in rete "end-to-end" tra software e hardware (processo tecnologico) e il software come capacità centrale dei sistemi d'arma (vantaggio operativo).

L'intelligenza artificiale troverà una prima applicazione come filtro veloce per l'analisi di quantità elevate di informazioni. Grazie a parole chiave nelle comunicazioni o il rilevamento nelle immagini si può ridurre l'impiego di personale, utilizzandolo in modo più efficiente e a beneficio delle attività di condotta e di comando.

Il Cdo Ciber è in fase di realizzazione: le azioni nello spazio ciber sono parte integrante di ogni conflitto attuale, non solo a partire dallo scoppio di un conflitto armato, ma già giornalmente. Il Cdo Ciber forma così, in modo figurato, una prima linea di difesa, ma si trova in una situazione eccezionale, una "chance come l'allineamento dei pianeti in astronomia". La logica di fusione dei dati dell'F-35, il Cdo Ciber nella medesima direzione con la nuova piattaforma numerica e gli altri strumenti, oltre all'integrazione delle Forze terrestri permetteranno all'Esercito svizzero "di ottenere una superiorità nel sapere e nella presa di decisione, in caso di guerra, ma non soltanto". ◆