Zeitschrift: Rivista Militare Svizzera di lingua italiana : RMSI
Herausgeber: Associazione Rivista Militare Svizzera di lingua italiana
Band: 96 (2024)
Heft: 6

Artikel: La Brigata d'aiuto alla condotta 41/SIS tra Comando Ciber e destinatari delle sue prestazioni
Autor: Annovazzi, Mattia
DOI: https://doi.org/10.5169/seals-1074881

La Brigata d'aiuto alla condotta 41/SIS tra Comando Ciber e destinatari delle sue prestazioni

col
Mattia Annovazzi

colonnello Mattia Annovazzi

Giovedì 22 agosto 2024 presso il Campussaal Brugg-Windisch, il br MARTINO GHILARDI ha presentato l'attività della brigata, di cui è al comando dal 1° aprile 2023.

Parte prima

Dopo una retrospettiva ad ampio raggio degli impieghi e dell'istruzione svolti nel 2024 dalla grande unità (tra gli altri, WEF, Patrouille des galciers, "PILUM", esercitazione Lockshield, Conferenza del Bürgenstock, corsi e preparativi di pianificazione per "telecomunicazione Esercito") ha sottolineato l'importanza di fruire di una legittimazione generale e quindi poter disporre della necessaria libertà di manovra per riuscire a fornire al meglio le prestazioni richieste.
Il futuro della brigata va visto in rapporto ai conflitti moderni, che si inseriscono in un radicale cambiamento caratterizzato dalla politica di potenza e dalla regionalizzazione dei conflitti con nuovi grandi attori. Nonostante una crescente messa in rete a livello economico, l'intensità dei conflitti è in crescita, con il rischio che lo stato di diritto basato sulle regole abbia la peggio sul "diritto del più forte". Gli stati europei e i loro eserciti si chiedono come affronteranno le minacce e i pericoli futuri e in che misura gli Stati Uniti continueranno a svolgere un ruolo di garante se dovesse legare le sue forze nel pacifico. "Come Svizzera, Esercito e Grandi Unità dobbiamo occuparci della questione".

Dall'esame sull'asse temporale dei meccanismi esistenti, della dottrina e delle tattiche si possono dedurre le misure per le proprie truppe.
La via verso il ritorno alla capacità di difesa si articola su più anni ed è in sé semplice. Nel 2029 ci sarà la prossima riforma dell'organizzazione dell'esercito in cui è possibile inserire misure precise sulle strutture dell'Esercito e sulla legislazione, con le relative implicazioni sul personale e il materiale. Nel 2026 occorre fornire i primi elementi. Nel 2029 molti militi di milizia o professionisti non saranno più attivi, ma questo rimane il focus. Alla fine del 2026 occorre avere una solida concezione della grande unità nel futuro a livello strutturale, personale e materiale, al fine di potersi muovere con successo "sul terreno di battaglia".
Alla base ci sono i meccanismi delle procedure d'impiego (*Einsatzverfahren*); il

resto come il materiale e il personale, è la conseguenza e segue. Il piano orario è quindi focalizzato al 2026.

Occorre tuttavia una precisa e approfondita conoscenza della propria formazione. La brigata non è una formazione omogenea ed è piena di sfaccettature, che possono essere messe a fuoco grazie ad alcuni criteri.

- Intercambiabilità tra componenti professionali e di milizia: le formazioni possono portare le prestazioni in modo complementare o esclusivo. Esclusività solo dalla milizia, mentre per le organizzazioni professionali non in modo autonomo per mancanza di capacità o conoscenze. All'elemento professionale viene assegnato il compito in generale, l'istruzione e l'accompagnamento della truppa.
- Complementarietà significa che l'organizzazione professionale viene rinforzata dalla milizia. La capacità di durata in un'una certa fase o una capacità in un certo ambito vengono aumentate. La formazione di milizia non è in grado di fornire la prestazione autonomamente. All'organizzazione professionale incombe di fatto l'integrazione della condotta e dell'assolvimento della prestazione in modo dettagliato. Il passaggio dall'esclusività alla complementarietà avviene in modo fluido e non va intesta in modo assoluto; forme miste sono possibili. Complementarietà ed esclusività non vanno intese in modo cognitivo, ma sono in rapporto di concorrenza.
- Le prestazioni avvengono per expertise individuale o attraverso un processo di lavoro collettivo. Singole persone o piccoli gruppi portano a un livello complessivo, in parte si completano e si integrano in capacità già esistenti, in parte in capacità aggiuntive. Expertise collettiva significa che la prestazione può essere portata soltanto da una formazione, come pure la capacità di durata.

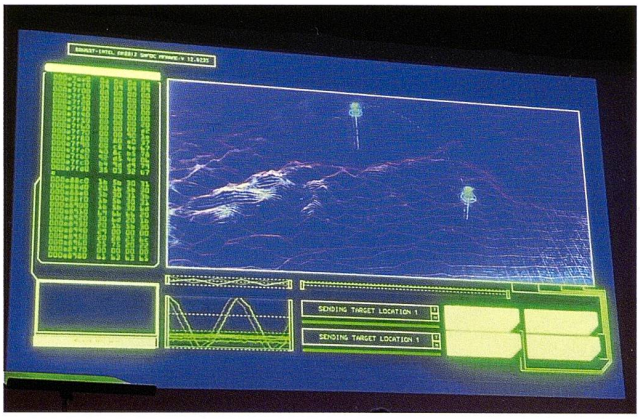
Le formazioni possono essere valutate nel rapporto con la brigata nel loro complesso. La rilevanza della grande unità si misura sulla conduzione della stessa. In generale, attraverso tutte le sue formazioni, la brigata assume responsabilità a livello tattico e tecnico-militare.

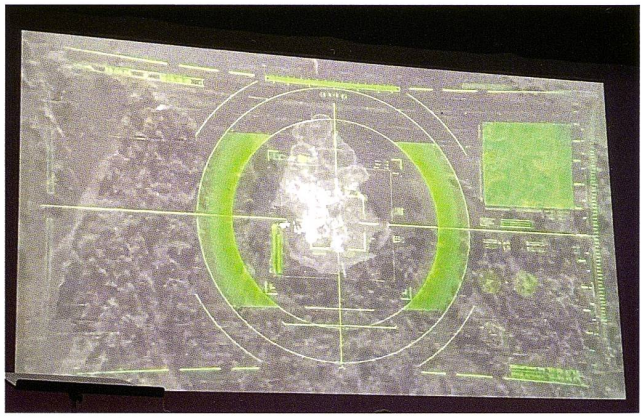
Per quanto riguarda le procedure di impiego, più è piccola la formazione impiegata nella realtà e meno si caratterizza per elementi di natura tattica. Il livello tattico è quello a livello unità/cp fino a grande unità. Al di sotto di questa soglia non ci sono procedure di impiego e si rimane a livello tecnico. Condurre la brigata significa farlo a livello tattico: il focus sta nella messa in rete e in relazione di persone, mezzi e capacità. La condotta tecnica rimane presso le unità direttamente subordinate al Cdo Cyber (formazioni professionali). Agire come *force providing* significa che la brigata primariamente mette a disposizione il personale necessario, anche a livello amministrativo. La costruzione tattica (senza le procedure di impiego) è compito delle formazioni professionali e tecniche.

La minaccia va compresa in modo concreto e si ripercuote nelle procedure di impiego delle singole formazioni. Nella minaccia il focus è il "settore attaccabile". Un'immagine di partenza la otteniamo se a fianco delle forme di conflitto moderno abbiamo una comprensione profonda delle nostre truppe. L'immagine della minaccia sorge quale conseguenza delle singole minacce individualizzate a livello di corpi di truppa. Una prima versione del catalogo delle minacce 2023 è stato trasmesso ai corpi di truppa.
Per la brigata rappresenta una minaccia (1) tutto quanto proviene dalla terza dimensione, (2) tutto lo spettro delle minacce a livello cibernetico ed elettromagnetico (CER), anche se al momento l'attenzione è rivolta maggiormente in ambito elettromagnetico e (3) i piccoli gruppi di fanteria. "Ci possono trovare e colpire se rimaniamo statici e se ci ammassiamo". Ci sono poi differenze di esposizione sull'asse temporale tra i vari corpi di truppa. È importante che l'immagine della minaccia dei beneficiari delle prestazioni non sia ripresa 1:1, ritenuto che le differenze possono essere anche molto marcate.

Le truppe informatiche mobili delle forze armate tedesche

Il col SMG Jürgen Schweiger, Kommando Informationstechnik-Services der Bundeswehr (Kdr ITTr KdoIT-SBw) ha presentato truppe e mezzi a livello di tecnica dell'informazione della Bundeswehr.





Queste truppe attraverso la radio, la comunicazione satellitare, il sistema di comunicazione digitale mobile, la tecnologia di rete, dei server, della comunicazione mobile criptata e del ponte radio digitale garantiscono la gestione in rete e la comunicazione fluida in Germania e nelle aree operative della Bundeswehr, fornendo parti della rete di comunicazione e applicazioni centralizzate e decentralizzate per gli utenti. Sono in grado di elaborare, trasmettere e gestire le informazioni mediante potenti sistemi informatici all'avanguardia. Assicurano in modo affidabile la capacità di comando e controllo ("connessione informatica globale") della Bundeswehr durante le missioni all'estero, grazie anche a personale altamente qualificato. In patria, forniscono supporto in caso di disastri naturali e incidenti particolarmente gravi, nonché durante i programmi di addestramento. Senza queste truppe, le forze mobili e stazionarie non sarebbero in grado di controllare e coordinare un'operazione su lunghe distanze.

In relazione a sfide e minacce, ha menzionato il problema dell'uso dei social o di applicazioni (smartphone e uso intuitivo) da parte delle truppe, perché rivela gli stazionamenti militari al nemico (ad es. soldati hanno usato un'applicazione per jogging [Fitnesstracker] durante una missione all'estero; ciò ha permesso di mappare attività e stazionamenti militari, oltre a informazioni). "Occorre creare una consapevolezza di ciò che trasmettiamo nello spettro elettromagnetico". Anche La NATO svolge attività di *Open Source Monitoring* durante le esercitazioni (ad es. in Trident Juncture Exercise). La crittografia "consuma" larghezza di banda che già oggi non basta. Ritengono già oggi di essere troppo lenti sul campo di battaglia, a partire dagli spostamenti. Contro i droni occorrono mezzi di difesa antiaerea. I centri di calcolo (nei bunker) sono tendenzialmente statici/stazionari, ciò che va migliorato. In caso di difesa o di crisi, non è chiaro quale validità avrebbero ancora contratti/accordi stabiliti ad esempio con i provider (IT-Services, contratti di lavoro e termini di disdetta ecc.). "Se chi porta un'uniforme è *kriegstauglich* altro discorso è sapere se è *kriegstüchtig*".

Anche con riguardo alla gestione di crisi a livello internazionale, "la digitalizzazione è l'autostrada per giungere nei settori di impiego" (NATO fianco est e Landes- und Bündinisverteidigung LV/BV).

Se si getta uno sguardo all'Ucraina, le supposizioni fatte hanno potuto essere confermate sul terreno, quando non rinforzate. L'inadeguata consapevolezza dei sistemi IT porta a enormi svantaggi nella gestione delle operazioni e mette a rischio le proprie truppe. Sono state constatate mancanze a livello di rete *end-to-end*, di crittografia, di passaggio (non) consapevole di informazioni attraverso l'IT privata (telefonate). Molteplici minacce all'infrastruttura stazionaria/dispiegabile sono generate, direttamente, attraverso attacchi cinetici e operazioni informatiche e, indirettamente, ad

esempio per la mancanza di personale operativo o di elettricità.
L'integrazione di fornitori civili genera vantaggi nella fornitura di servizi, ma anche svantaggi se porta a dipendenze.

Il tema della capacità di comunicazione è molto presente nella Bundeswehr. Boris Pistorius, ministro della difesa tedesco ha definito queste capacità come "occhi, orecchie e sistema nervoso delle forze armate". Occorre mettere a disposizione le informazioni sul terreno nei tempi necessari. Il quadro che si poteva osservare soltanto in Afghanistan è cambiato. Ritenuto il presupposto che nel 2029 la Russia sarà in grado di attaccare la NATO, intendono terminare gli aggiornamenti entro il 2027. In Germania si discute se reintrodurre l'obbligo di servizio viste le necessità in personale che ci saranno nei prossimi anni.

La direzione intrapresa è quella di disporre di "punti di erogazione del servizio" (*Service Delivery Point:* Connessione/Collegamento in rete/ Funzionamento) con le seguenti caratteristiche.
- Possono essere installati e utilizzati in modo indipendente, in variante "large" per grandi installazioni/maggiore larghezza di banda o in variante "small" per sensori di piccole/medie dimensioni/larghezza di banda inferiore.
- Forniscono l'accesso alla rete centrale.
- Consentono la fornitura di servizi IT nella rispettiva area di responsabilità.
- Collegamento in rete con altri punti di controllo.
- Controllano e monitorano i sistemi IT collegati.

Al momento la Bundeswehr dipende da troppi servizi IT (e-mail ecc.) e nei prossimi anni intende ridurne il numero in modo importante. "Dietro a un servizio IT c'è un provider [fornitore] e dietro ai provider ci sono delle persone che oggi non ci sono".

Attualmente la Germania, in questo ambito, dispone di 6 bat e 1 direttamente subordinato alla NATO. Nel documento *NATO 2022 Strategic Concept* sono state ribadite le missioni chiavi che sono la deterrenza e la difesa, la prevenzione e la gestione delle crisi, la sicurezza cooperativa. L'approccio a 360° è stato mantenuto, mentre la Russia da partner è stato qualificato come minaccia per la sicurezza europea. Nella *riforma 2025+* il dispositivo sarà adeguato e rafforzato. Il *New Force Model*, sistema di prontezza NATO, prevede attualmente 100 000 mil entro 10 giorni, 200 000 entro 30 giorni, 500 000 entro 180 giorni. La Germania contribuisce con 14 200 mil e 34 aerei e navi nella *NATO response force* (fino al 2024). Dal 2025 sono previste attribuzioni regionali. La Germania contribuirà con 30 000 militi e 85 aerei e navi. Metterà a disposizione 3 bat. Sulla base delle decisioni prese all'incontro della Nato a Madrid la Germania ha emesso le *Verteidigungspolitische Richtlinien 2023.*
Le missioni centrali della difesa nazionale e dell'Alleanza (LV/BV) concernono:
- Misure di dissuasione nei confronti di potenziali avversari sia sul territorio tedesco sia su quello dell'Alleanza in tutte le dimensioni;
- Compiti di difesa sul territorio tedesco, compresa la difesa territoriale nazionale;
- Difesa dagli attacchi sul territorio dei partner dell'Alleanza;
- Difesa contro le minacce terroristiche e ibride;
- Rafforzamento delle capacità di difesa transatlantiche ed europee.

La preparazione alla guerra (*Kriegstüchtigkeit*) è divenuta il principio guida: l'ambizione è quella di poter disporre di soldati che hanno la volontà di difendere coraggiosamente i diritti e la libertà del popolo tedesco, accettando consapevolmente il rischio della vita e dell'incolumità fisica.

Parte seconda

Il br Martino Ghilardi ha continuato la sua esposizione, ricordando che il rafforzamento della capacità di difesa si basa su un'immagine approfondita e concreta della minaccia.
Le procedure di impiego della brigata in futuro si caratterizzeranno per alcuni criteri. Si tratta di procedere possibilmente in piccole formazioni, evitando ammassamenti così da non diventare facili obiettivi. Si tratta di ottenere un massimo di camuffamento possibile in tutti le dimensioni, in particolare a livello elettromagnetico, in modo da non venir reperiti. Si tratta di ottenere un'alta mobilità in modo da sottrarsi all'esplorazione e alle forze dell'avversario.

Non si può lavorare in modo isolato. L'integrazione dei processi della Br aiuto cond 41 con il Cdo Ciber e le necessità di coordinazione con le truppe combattenti (destinatari delle prestazioni) vanno implementate. Le procedure di impiego devono essere fattibili e istruibili. La costruzione e l'elaborazione di nuove procedure di impiego presuppone una comprensione profonda della minaccia e della propria truppa. Non significa negare le implicazioni di un avversario fuori dai settori di impiego di competenza, al contrario: a causa della possibilità di escalation, della precisione e della velocità, minacce usuali di natura fisica divengono più pericolose.

Nel 2024 sono state fatte le prime prove a livello di meccanica di mobilità, con lo scopo di creare maggior velocità dove possibile. Nel 2025 i battaglioni si chineranno sul pilotaggio e la condotta, per legare il tutto. Una mezza sezione per c trp svolgerà il compito di *Lenkungsstelle*. Il grosso della truppa fino al 2026 lavorerà secondo le procedure di impiego che hanno dato buona prova sino ad ora, ma con pazienza si tenderà ai nuovi obiettivi per permettere una crescita, così da non ingenerare confusione e frustrazione. Idealmente nel 2026 l'impiego potrà essere testato con cp mobili, "senza essere già veloci e perfetti", ma nell'ottica di verificare la correttezza dei concetti.
Lo scopo è poter indicare gli elementi per la revisione del 2029. Inoltre, lo scaglione superiore e i destinatari delle

prestazioni (truppe combattenti) verranno coinvolti "in rete".
I primi tentativi a livello di truppa partiranno nella primavera del 2025.

Oltre alla eterogeneità tra milizia e professionisti, è importante considerare la *consistenza della tecnologia in un'ottica "end-to-end"*. Le infrastrutture permanenti del Cdo Ciber sono in parte realizzate e si compongono di nodi a livello nazionale con centri di calcolo, nodi a livello regionale e la rete di condotta, che è una sorta di autostrada per i dati. Il grosso del Cdo Ciber è nelle infrastrutture permanenti. La brigata è prima di tutto in impiego sul terreno. La prestazione di combattimento può riuscire soltanto se tutti gli attori agiscono insieme. Se l'ambito "Einsatz IKT" rispettivamente il CESA (Cyber und elektromagnetische Sicherheit und Abwehr) non mettono a disposizione i dati; se i gruppi ondi non trasportano i dati e il gruppo CESA non sorveglia e protegge i sistemi in modo permanente, la brigata non può adempiere le proprie prestazioni. Tanto meno se la brigata non riesce a impiegare i sensori e gli effettori oppure "nell'ultimo miglio" la trasmissione di dati non riesce ai destinatari della prestazione. Naturalmente ci sono limitazioni "logiche" per la realizzazione. Per l'impiego tattico e militare del compito tecnico è la brigata che è competente. "La brigata è una componente integrante del Cdo Ciber e non una formazione autonoma in senso classico del termine", ha concluso il br Ghilardi.

Un aggiornamento dal Cdo Ciber

Impressionante la presentazione del div Simon Müller, capo del Cdo Ciber dell'Esercito svizzero.
Nella guerra contro l'Ucraina, la dimensione cibernetica viene utilizzata principalmente per operazioni informative o attacchi tattici ai mezzi di comunicazione che servono principalmente a scopi militari. *Gli attacchi informatici accompagnano gli attacchi cinetici per amplificarne gli effetti*. Ad esempio, i mezzi informatici possono essere utilizzati per interrompere a breve termine le comunicazioni o bloccare le infrastrutture delle organizzazioni "luci blu" nell'area bersaglio, al fine di rallentare l'assistenza "a valle" (v. Sicurezza Svizzera 2023, Rapporto sulla situazione del Servizio delle attività informative della Confederazione). Importante rilevare che l'elemento cibernetico viene utilizzato prima, durante e dopo un conflitto a scopo di destabilizzazione. Peraltro, non è semplice distinguere tra criminalità cibernetica e altre forme di azioni.

I *malware* in Ucraina hanno cagionato danni per 10 mia di franchi. Ciò è rilevante anche per la Svizzera, se si pensa al caso Xplane da un'altra prospettiva: la fiducia nello Stato svizzero si incrina. Con i *ransomware* vengono pubblicati dati che riguardano persone, quindi rilevanti sotto il profilo della necessaria protezione. Il messaggio è: "è stato trovato un punto debole, è stato utilizzato, abbiamo raggiunto informazioni rilevanti che non siete stati in grado di proteggere". Questi dati possono risalire anche di parecchi anni nel passato. Le interazioni di forme di attacchi cibernetici e campagne di disinformazione sono percepite dalle controparti, mentre gli autori restano al coperto. Se si considerano le risorse importanti che vengono messe a disposizioni negli altri paesi (possono essere anche di 10 volte superiori alle nostre) o da noi non ci sono problemi o i sistemi sono già stati violati senza che ce ne si sia accorti. La protezione cibernetica serve quindi già prima dei conflitti per evitare di subire tentativi di destabilizzazione.

La Svizzera è oggetto di attacchi? Dipende dall'interesse degli attori in campo. Ad esempio in Polonia gli attacchi aumentano con l'avvicinarsi dei Russi al loro paese.
Possibili conseguenze della guerra per la Svizzera in ambito cibernetico sono
- attacchi informatici per campagne di disinformazione contro persone/istituzioni svizzere (piuttosto probabili);
- campagne di disinformazione attraverso l'hacking di obiettivi stranieri che hanno influenza sulla formazione delle opinioni e sulle posizioni svizzere (probabili);
- spionaggio informatico contro la Svizzera (molti probabile).

Grazie alla *rete integrata sensori-servizio informazioni-condotta-effetti* (SNFW), l'obiettivo perseguito è di poter decidere più velocemente della controparte, o accelerando il processo, o disturbando quello dell'avversario. Questo è il compito del Cdo Ci. Le capacità operative della digitalizzazione contribuiscono ad accelerare il processo, le azioni nello spazio cibernetico ed elettromagnetico disturbano il nemico. Le misure di autoprotezione (CER) servono ad impedire di essere disturbati, proteggendo le formazioni di truppe, i sistemi, le infrastrutture, le informazioni e le reti della CER dalle interferenze di un avversario.

Dove sono i *pain points* attualmente?

– *Mezzi di comunicazione, ovvero trasporto di dati, mobilità parziale o completa.* L'F-35 è in sé un SNFW chiuso, quindi occorrono comunicazioni e trasporto di dati. Se si è deboli qui ad ogni passo vi è un ritardo. Il progetto TC Es (TK A) – i cui componenti saranno installati praticamente in ogni piattaforma di veicolo o corpo di truppa, sia che si tratti di radio, raggi direzionali o della sostituzione del Sistema Integrato di Telecomunicazioni Militari (SITM) – dovrà fornire una soluzione. "Tuttavia, oggi siamo entrati nella famiglia dello F-35. Lo strumento TC Es in sé ha i suoi pregi, ma la velocità di 2.5 Kbit/s non basta. Con un fattore mille e oltre, siamo a un altro livello". Le procedure vanno adattate e occorre sfruttare le possibilità offerte dal progresso tecnologico. La radio tattica a suo tempo era un ottimo strumento mobile per la trasmissione simultanea vocale. Oggi non è più un sistema rilevante. Occorre esaminare tutta la gamma dei sistemi, visto che TC Es è in ritardo e a livello civile ci sono già soluzioni come *mobile satcom* o altri. La sfida per l'Esercito è introdurre sistemi in modo tale che tra 10 anni non si debba iniziare tutto dall'inizio. In relazione a tutta la trasformazione digitale occorre ben riflettere dove introdurre cosa.

– *Passaggio e migrazione dei dati tra sistemi* come FIS Heer, FIS LW, Intaff per la condotta del fuoco ecc. Ogni sistema è isolato, ha una piattaforma separata e distinta. Per scambiare i dati è un problema: non posso trasmettere o trasformare direttamente i dati, ma occorrono *memory stick* o altre soluzioni ciò che "non è veloce". La soluzione qui sarà la *nuova piattaforma digitale (NDP)* per tutte le applicazioni. Questa piattaforma IT diventerà la base per la condotta dell'Esercito svizzero a terra, nell'aria, nello spazio, nel ciberspazio, nello spazio elettromagnetico e nello spazio informativo. Tutti i mezzi di ricognizione (droni, radar ecc.), i sistemi d'arma, di "comando e controllo", le truppe sul campo saranno collegati in rete digitalmente tramite questo sistema. Il problema è che portare i sistemi d'arma e hardware/

software esistenti o pianificati sulla nuova piattaforma digitale costa denaro, tempo e risorse. Questo è anche il motivo per cui il nuovo sistema di sorveglianza aerea (Skyview) sta diventando due volte più costoso ed è attualmente sospeso. Occorre poi essere coscienti che l'industria degli equipaggiamenti non funziona con la logica auspicata, ma con sistemi proprietari o applicazioni. Si è però detto fiducioso per il futuro.
- *Autoprotezione CER:* il paesaggio dell'infrastruttura della comunicazione e della tecnologia è estremamente eterogeneo. Si parla di un migliaio di applicazioni. Occorre un approccio basato sul rischio, non potendosi proteggere tutto (*security by design*).

Non è importante disporre soltanto di materiale e mezzi finanziari, ma vanno sviluppate capacità attraverso l'aggiornamento di procedure di impiego o a livello organizzativo. Qui sono decisivi l'expertise personale e il *people business*. Ritiene di essere in una posizione di privilego perché a fronte di risorse limitate il CEs e la capa del DDPS riconoscono e appoggiano l'importanza di questo ambito. Nella difficile situazione attuale, il personale ha potuto essere aumentato e le competenze ampliate. Nonostante ciò c'è un ambito in cui non si può raggiungere ciò che si vorrebbe, ovvero nelle azioni nello spazio elettromagnetico, nel senso che ogni unità possa condurre delle azioni autonomamente. A causa del quadro finanziario questo obiettivo attualmente non può essere raggiunto.
Il profilo di prestazione che si vuole ottenere con il Cdo Ciber è di riuscire a difendere ben prima che inizi un attacco cinetico. Quindi va chiarito quale sia il funzionamento e il coordinamento con la SEPOS, l'Ufficio federale della protezione della popolazione, l'Ufficio federale della cibersicurezza, il Servizio delle attività informative della Confederazione. È un cantiere in corso.

Le prestazioni di digitalizzazione sono effettuate nei nodi a livello nazionale, la sorveglianza di sicurezza è centralizzata, le azioni sono svolte prima di tutto centralmente: questa impostazione di centralità è quella più efficiente. L'interoperabilità con partner nazionali e internazionali (PESCO, Cyber Range Federation ecc.) è importante. "Non si tratta di alleanze ma di sviluppare capacità per poter collaborare". Nell'ambito cibernetico è convinto che la sicurezza si crea con la messa in rete e lo scambio di informazioni. In caso di escalation occorre poter intensificare le prestazioni in una "zona di sforzo principale", con i collegamenti ma anche in modo decentralizzato tramite piccoli centri di calcolo (edge computing ecc). Se un nodo dovesse cadere, il successivo coprirebbe la lacuna, in modo da restare "robusti". Un secondo centro di calcolo (CASTRO 2) è previsto nel messaggio sull'esercito 2024. Occorre essere resilienti. La sorveglianza sulla sicurezza deve poter essere decentralizzata.

Cosa interessa ai partner internazionali quando visitano la Svizzera? L'aumento della disponibilità; da 700 collaboratori si può arrivare a 11 000 (milizia) e questo in combinazione con i partner. Molti paesi hanno rinunciato a questa capacità.
Da rilevare che non si risolve tutto con i mezzi tecnici. Ad esempio nell'esercizio PILUM la messa a disposizione di un ufficiale di collegamento del Cdo Ci ha permesso di migliorare la coordinazione. È fiero del centro operativo di condotta del Cdo Ci anche se non funziona ancora come dovrebbe, ma è importante averlo. La Base d'aiuto alla condotta (BAC) non disponeva di un ambito fondamentale di condotta a livello di informazioni (AFC 2), quindi a livello di anticipazione non poteva agire a seconda della minaccia.
A lungo termine da citare la costruzione di capacità a livello di *data science* e IA (DALFi-V) che si inseriscono tra la comprensione della situazione, la condotta in collaborazione e un'elaborazione dati robusta e sicura. Da rilevare anche lo sviluppo in corso e nei prossimi anni di servizi centrali a livello Esercito (Cyber Fusion Center [CFC] operativi e di sorveglianza di sicurezza di sistemi critici per l'impiego) di servizi decentralizzati CFC con capacità incrementali, di Mission Defence Teams (MDT) e di Cyber Rapid Reaction Teams (CRRT).

Comprendere la situazione nella rete, identificare i rischi e le minacce, comprendere il contesto e riconoscere le opportunità e valutarle in modo coerente quando si lavora insieme, elaborare i dati in modo sicuro e robusto e distribuirli in linea con ordine e in ogni situazione, disporre di una leadership organizzativa e tecnica nella rete e garantire la gestione organizzativa e tecnica a tutti i livelli e in tutte le sfere operative in collaborazione con i partner: sfide di grandissima e prioritaria rilevanza per il sistema paese che il Cdo Ci saprà vincere, sempre che sia messo in condizioni di poterlo fare.

◆


LA SICUREZZA È anche DONNA
Milena
Melanie
Joëlle
Anika
Janine
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Esercito svizzero