Zeitschrift: Rivista Militare Svizzera di lingua italiana : RMSI
Band: 90 (2018)
Heft: 6

Artikel: Combattere, proteggere e aiutare, anche nel ciberspazio
Autor: Annovazzi, Mattia
DOI: https://doi.org/10.5169/seals-846907

Combattere, proteggere e aiutare, anche nel ciberspazio

L'Esercito protegge costantemente i propri sistemi d'informazione e comunicazione da attacchi cyber, impiegando parti dell'organizzazione di professionisti della BAC, appoggiati da militari di milizia dell'Esercito altamente specializzati.

colonnello Mattia Annovazzi

L'Esercito e il ciberspazio

La memoria corre forzatamente a un paio di anni fa, quando si seppe che hacker erano riusciti a penetrare la rete della RUAG, sottraendo più di 20 gigabyte di dati. Fu uno degli attacchi cyber più importanti in Svizzera, rimasto per lungo tempo sconosciuto. Il caso fece comprendere al Consiglio federale – finalmente – che l'Esercito svizzero in ambito di sicurezza IT era sottodotato. Ciò accelerò il Piano d'azione Cyber-Defence, partito con le riflessioni sull'USEs, che dovrebbe essere realizzato entro il 2020. I collaboratori in ambito di sicurezza IT saranno tripilcati, fino a raggiungere le 150 unità.

Al più tardi dal 2014, la NATO ha riconosciuto il ciberspazio come "dimensione" autonoma. Nella dottrina militare svizzera si parla di "sfere operative" intendendo "aria [incluso lo spazio interplanetario], suolo [incluso lo spazio marittimo], settore elettromagnetico, cyberspazio e settore delle informazioni" (v. Estratto COSM 17 per ufficiali subalterni, Documentazione 50.040.03 i, n. 122). Il riconoscimento del ciberspazio – con la sua stratificazione *fisica* (materiale), *logica* (informazioni e istruzioni ai sistemi) e *sociale* (elaborazione di dati) – ha permesso agli Stati di mobilitare importanti mezzi finanziari e ha costituito lo stimolo a occuparsene e a parlarne, già solo per motivi di prestigio.
Il lato implementativo/realizzativo è, tuttavia, ben altra cosa. I contorni della minaccia cyber appaiono ancora incerti, sia sotto il profilo della sua rilevanza, sia delle forme in cui in futuro potrà manifestarsi. In ogni caso questa minaccia non è più eludibile o confinabile in ambiti o settori specifici. Il potenziale innovativo e l'elevato grado di adattabilità pongono sfide cruciali anche all'Esercito, già solo su come strutturare un'organizzazione con queste caratteristiche e su come mettere a frutto le conoscenze cyber. Gli armamenti sono sempre più costituiti da software e meno da hardware, ragione per cui la guerra in rete pervade ormai tutti gli aspetti della condotta di operazioni, dell'approvvigionamento, della gestione della truppa, in un quadro globale, e del trattamento dell'informazione, già in tempo reale.

Le *forme di ciberminaccia* possono essere suddivise nelle categorie
- vandalismo
- attivismo
- criminalità
- terrorismo
- conflitto.

Lo spionaggio precede le altre forme di minaccia con intensità crescente. Di regola, non è possibile riconoscere una chiara distinzione tra queste categorie.

Gli attori nel campo delle ciberminacce sono raggruppati in modo sommario in cinque livelli:
- M1: utilizzatori di strumenti, tools, per hacking;
- M2: sviluppatori di vulnerabilità, hacker motivati;
- M3: organizzazioni professioniste, cibercriminali;
- M4: agenti di minaccia irriconoscibili e spazializzati;
- M5: ciberpotenze.

La complessità degli attacchi e il know-how necessario aumentano in modo progressivo a seconda della categoria. Per contro, diminuisce la probabilità di essere colpiti e di subire un danno.

L'Esercito deve poter garantire in ogni momento e in qualsiasi situazione *le proprie capacità operative e la libertà d'azione* anche in questa sfera operativa. L'Esercito deve essere costantemente in grado di riconoscere le ciberminacce, di proteggersi da esse e di combatterle. Ne deriva la necessità di articolare e implementare processi di *condotta*, di *anticipazione*, di *prevenzione* e di *reazione*. In caso di conflitti, l'Esercito deve essere in grado di appoggiare le operazioni militari con azioni cyber.

Sarebbe scorretto affermare che l'Esercito si occupi solo ora di ciberspazio, ritenuto quanto fatto dal DDPS già a partire dagli anni 2000. Le iniziative dell'Esercito in campo cyber riguardano il programma FITANIA (infrastruttura di condotta, tecnologia dell'informazione e collegamento alla rete dell'esercito) oltre allo sviluppo di competenze cyber, con lo sviluppo di capacità, la creazione di 64 posti di specialisti per consolidare l'organizzazione e l'aumento degli effettivi dei quadri e dei soldati di milizia a circa 600 unità. L'investimento previsto è di circa 4 miliardi di franchi.

Le 7 regole

- Considerate sempre pubbliche le dichiarazioni nei social media.
- Mai collegare apparecchi USB sconosciuti o privati a sistemi dell'esercito o dell'amministrazione.
- Hotspot pubblici possono essere dannosi. Un hotspot con il proprio smartphone è più sicuro.
- WLAN, Bluetooth, GPS, NFC sono disattivati, a meno che non siano coscientemente necessari.
- Cellulari, orologi e notebooks sono potenzialmente delle cimici. Prima di conversazioni confidenziali o segrete riponete altrove questi apparecchi.
- Non aprite messaggi/allegati/link di provenienza inattesa. In caso di dubbio contattate il mittente telefonicamente.
- In caso si sospetti un'infezione da malware, interrompete il prima possibile il collegamento alla rete, lasciate il sistema in funzione e comunicate i vostri sospetti alla hotline e al vostro superiore.

La novità è, invece, che si punti sulla milizia. Molti eserciti vivono un manco di personale in questo ambito, causato dalla concorrenza con l'economia privata, in cui vi sono prospettive di carriera e remunerazione migliori. L'approccio tipicamente elvetico potrebbe permettere di contenere il problema.

Il corso di formazione per reclute cyber

Ai primi di agosto di quest'anno, 18 reclute hanno iniziato il primo corso di formazione cyber, che è stato concepito e realizzato dall'Esercito e dai suoi partner in meno di un anno. Nella giornata di presentazione – svoltasi il 21 settembre 2018 presso la Scuola di guerra elettronica 64, sulla piazza d'armi di Jassbach tra il Berner Oberland e l'Emmental – i responsabili hanno tracciato un bilancio intermedio positivo. Si tratta di un'importante pietra miliare nell'ambito del Piano d'azione Cyber Defence, per rafforzare l'ambito della ciberdifesa dell'Esercito svizzero.

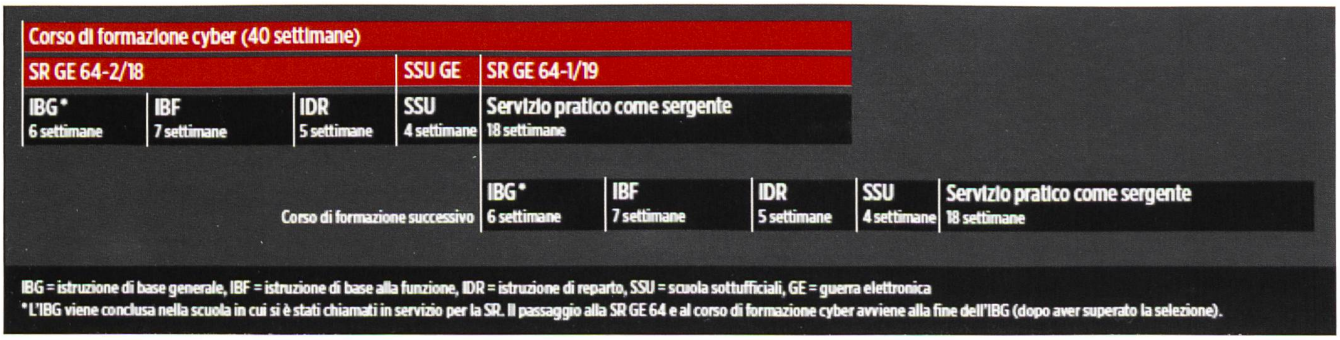
Il **comandante di corpo Philipp Rebord**, capo dell'Esercito, ha incentrato il suo intervento sulla milizia e sulla *situazione win-win* venutasi a creare per l'economia e l'Esercito. L'Esercito può trarre vantaggio dalle conoscenze di cui le giovani reclute già dispongono. Con il corso di formazione cyber si offre poi un perfezionamento anche a vantaggio dell'economia e più tardi, nei corsi di ripetizione, l'Esercito può approfittare delle esperienze professionali civili dei soldati cyber.

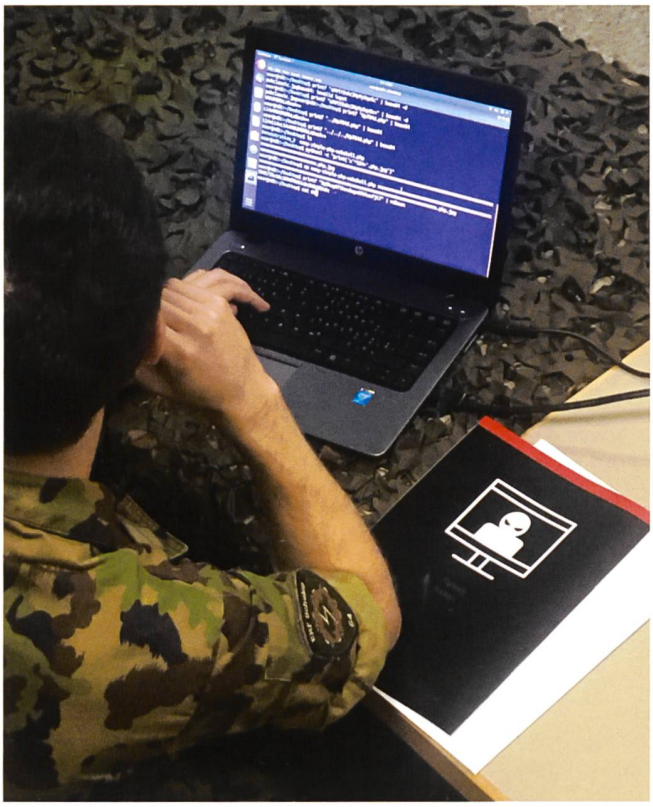
Il **divisionario Thomas Süssli**, capo della Base d'aiuto alla condotta (BAC) ha ricordato quali sono i compiti e i mezzi dell'Esercito nel ciberspazio.
La BAC è il fornitore di prestazioni nel settore delle tecnologie dell'informazione e della comunicazione (TIC) a favore del DDPS in ogni situazione: nella situazione normale e in caso di crisi, catastrofi o conflitti. A tale scopo la BAC gestisce una rete di comunicazione autonoma, che consente lo scambio sicuro di qualsiasi tipo di dati, per cui s'impone in permanenza un'elevata sicurezza e disponibilità. La BAC gestisce il *Centro per le operazioni elettroniche* (COE) che raccoglie informazioni per il Servizio delle attività informative della Confederazione. Si occupa anche della difesa da attacchi provenienti dal ciberspazio, della guerra elettronica (*Computer Network Operation*, CNO) e della crittologia. La BAC gestisce il *Computer Emergency Response Team militare* (milCERT), che è responsabile della sorveglianza delle infrastrutture TIC dell'Esercito. La BAC appoggia in prima priorità l'Esercito, ma anche la condotta politica e tiene a disposizione i mezzi adeguati. Dispone di uno stato maggiore di crisi.
Anche il divisionario Süssli ha sottolineato l'ottima collaborazione che si è instaurata e ha ricordato che nella seconda metà del 2019, nel quadro del corso di formazione, potrebbe essere già possibile dare l'esame professionale di *Cyber Security Specialist*, con attestato professionale federale.

Andreas Kälin, presidente dell'Associazione per la formazione professionale nell'ambito delle tecnologie per l'informazione e la comunicazione (TIC), ha presentato il certificato federale di *Cyber Security Specialist*, sottolineando che si tratta di un modello di successo basato su un progetto di partenariato pubblico privato, nell'interesse dell'economia, della società e dell'Esercito. Il profilo professionale sviluppato è il risultato di questo lavoro in comune.
La formazione TIC è la porta d'accesso principale per accedere a una formazione professionale superiore e nelle scuole specializzate fino al Politecnico federale, ma è anche la leva più importante per coprire i futuri bisogni di mano d'opera qualificata in questo campo.

Nella caserma di Jassbach, le reclute apprendono come proteggere le reti dell'Esercito in condizioni difficili, come bloccare quelle delle controparti, come scoprire (e difendersi da) attacchi che avvengono quotidianamente a reti di comunicazione sensibili dell'Esercito e di altre importanti infrastrutture del DDPS.
Questa "scuola reclute" dura circa 40 settimane e prevede 800 ore di formazione (basi generali 60 ore, basi tecniche 170 ore, istruzione trasversale 30 ore, formazione alla condotta 90 ore, istruzione specialistica 300 ore, impiego ed esercizi 150 ore).
Le reclute avanzano sino al grado di sergente.

Gli ambiti d'istruzione e i contenuti sono i seguenti:
- *Specialista Computer Network Operations* (CNO) – con compiti di sviluppatore di strumenti software, analista di avvenimenti e attacchi cyber, nonché analista di vulnerabilità.
- *Specialista milCERT* – con compiti di analista in un Security Operation Center (SOC), analisi di cyberminacce rivolte contro i sistemi tecnici informatici e di comunicazione dell'esercito, gestione degli incidenti e indagini tecniche, nonché forensi.
- *Specialista Cyber Defence* – con compiti di analisi e rappresentazione della situazione, appoggio (anche tecnico/forense), consulenza e istruzione di truppe sul terreno.





Durante la parte pratica della presentazione, è stato possibile assistere allo svolgimento di alcuni esercizi. Una recluta cyber ne ha spiegato scopi, modalità, particolarità e difficoltà.

Occorre motivazione e immaginazione per riconoscere le vulnerabilità e risolvere nei tempi richiesti questo tipo di esercizi, che si protraggono anche per molte ore.
È importante rilevare che le reclute non si allenano nella rete di comunicazione pubblica e che lo scopo dell'istruzione e le necessità dell'Esercito sono orientate alla difesa e alla neutralità elvetica. A più riprese è stato sottolineato che per poter garantire una certa capacità di durata l'Esercito dispone di circa 600 unità, che sono ripartite su 52 settimane annuali o a seconda delle necessità. Ogni soldato cyber svolgerà poi un'attività di spionaggio di segnali elettromagnetici (*SIGnals INTelligence*, SIGINT) per circa 20 giorni all'anno.

Se è vero che in Cina annualmente vengono formati circa 40 000 specialisti, è importante sottolineare che quanto fa la Svizzera si situa a un livello qualitativo elevato ed è rapportato alle sue necessità difensive e all'entità della sua popolazione. In base alla Legge federale sulle attività informative (LAIn), un eventuale ciberattacco è soggetto ad autorizzazione del Consiglio federale.
Per l'Esercito svizzero il primo corso di formazione cyber è un'importante pietra miliare nell'ambito della messa in atto del *Piano d'azione Cyber Defence* del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS), del novembre 2017.

Questo piano d'azione è orientato alla *Strategia nazionale per la protezione della Svizzera contro i cyber-rischi* che, tra l'altro, pone l'accento sulla responsabilità individuale di ogni singolo cittadino nel proteggersi da ciberattacchi e nell'affrontare le conseguenze. ◆

La strategia e le misure del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) per la protezione contro i cyberattacchi sono basate sulla *Strategia nazionale per la protezione della Svizzera contro i ciberrischi* (SNPC). Suo obiettivo è ridurre al minimo i ciberrischi grazie alla collaborazione tra le autorità, il mondo economico e i gestori di infrastrutture critiche.
La strategia indica, quali punti fondamentali per la riduzione dei ciberrischi,
(a) la *responsabilità individuale* (lo Stato deve intervenire solo quando sono in gioco interessi pubblici o nei casi in cui agisce in funzione del *principio di sussidiarietà*),
(b) la *collaborazione* tra economia, le scuole universitarie e autorità,
(c) la *cooperazione* con l'estero.
La strategia 2012–2017 include 16 misure. Il 18 aprile 2018 il Consiglio federale ha approvato la SNPC 2018–2023. Si basa sul lavoro della prima strategia, espandendola dove necessario e aggiungendo nuove misure.

La Strategia nazionale per la protezione della Svizzera contro i ciberrischi viene attuata in modo *decentralizzato*.

La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) – gestita in comune dall'Organo direzione informatica della Confederazione (ODIC) del Dipartimento federale delle finanze e dal Servizio delle attività informative della Confederazione (SIC) del DDPS – riveste un ruolo centrale. Il compito principale di MELANI consiste nell'individuare tempestivamente i ciberrischi e nell'aiutare i gestori di infrastrutture critiche (ad es. fornitori di energia elettrica, aziende di telecomunicazioni e banche) a prevenire e gestire questo tipo di rischi.
Dal 2004 il SIC offre il programma di prevenzione Prophylax, che mira a sensibilizzare il mondo svizzero dell'industria e della ricerca ai rischi costituiti dalle fughe di dati e dall'acquisizione illegale di informazioni.

L'*Esercito svizzero* svolge un ruolo fondamentale nell'attuazione dei provvedimenti per la protezione contro i ciberrischi. Come l'intera società, anche l'esercito si serve in larga misura delle tecnologie dell'informazione e della comunicazione e può dunque essere bersaglio di ciberattacchi. Per questo motivo deve innanzitutto proteggere le proprie infrastrutture e i propri mezzi. L'esercito investe in reti protette da attacchi e da pericoli di ogni genere e in questo contesto porta avanti i progetti "Centri di calcolo", "Telecomunicazione dell'esercito" e "Rete di condotta Svizzera".
Una volta che l'Esercito ha soddisfatto le proprie esigenze di protezione, in caso di bisogno può mettere le proprie capacità a disposizione delle autorità civili, in via sussidiaria, per la protezione contro ciberattacchi e contribuire così a mantenere funzionanti le infrastrutture critiche. In caso di conflitto armato l'esercito impiegherebbe tutte le sue competenze nel settore cyber per contrastare gli attacchi, ridurne l'efficacia e indebolire le capacità degli avversari in tale ambito.

La protezione della popolazione ha il compito di proteggere la popolazione e le sue basi vitali in caso di catastrofe, in situazioni d'emergenza e in caso di conflitto armato contribuendo così in misura determinante a limitare e gestire gli effetti di eventi dannosi. Nel quadro della Strategia nazionale per la protezione della Svizzera contro i ciberrischi (SNPC), l'*Ufficio federale della protezione della popolazione* (UFPP) esegue analisi dei rischi e della vulnerabilità relative a infrastrutture critiche. Sulla base di tali analisi l'UFPP elabora, unitamente alle autorità di regolazione, alle associazioni e ai gestori di infrastrutture critiche (ospedali ecc.), misure per migliorare la resilienza.
Per le autorità civili è indispensabile che i rispettivi sistemi di telecomunicazione e di allarme funzionino in qualsiasi situazione e che la popolazione possa essere preavvertita e allarmata attraverso canali sicuri, come pure che possa disporre di informazioni affidabili. A livello di Confederazione l'Ufficio federale della protezione della popolazione è impegnato in numerosi progetti volti a garantire reti di comunicazione a prova di crisi e di blackout.

All'interno del DDPS la *Sicurezza delle informazioni e degli oggetti* (SIO), che fa parte della Segreteria generale, è responsabile della protezione contro i ciberattacchi. La SIO si occupa della sicurezza integrale del DDPS. È competente in particolare per le direttive nei settori della sicurezza delle persone, delle informazioni, dell'informatica e dei beni (materiale e immobili).

Visto l'aumento dei ciberrischi, le esperienze di attacchi concreti e le nuove basi legali, nel 2016 il capo del DDPS ha deciso di verificare il dispositivo del DDPS per la protezione contro i ciberattacchi. A partire da tale verifica è stato elaborato un Piano d'azione Cyber Defence, che verrà attuato entro il 2020 di pari passo con la Strategia nazionale per la protezione della Svizzera contro i ciberrischi.


so quello
che voglio!
SIBYLLE EICHENBERGER | soldato d'ospedale
Le donne nell'esercito sono consapevoli,
impegnate e indipendenti.
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Esercito svizzero
www.esercito.ch/donne