



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Berna, 11 dicembre 2020

Esercito – Garantire le competenze nel settore delle nuove tecnologie

Rapporto del Consiglio federale in adempimento del
postulato 17.3106 Marcel Dobler del 14 marzo 2017

Indice

1	Situazione iniziale	3
2	Mandato	3
3	Competenze tecnologiche	4
3.1	Amministrazione	4
3.2	Base tecnologica e industriale rilevante in materia di sicurezza	5
3.3	Personale dell'esercito	6
3.4	Personale professionista militare e civile	8
4	Collaborazione con i partner	9
4.1	Istituti formativi	9
4.2	Economia privata	10
4.3	Cooperazione internazionale	10
5	Conclusione	11

1 Situazione iniziale

Lo sviluppo tecnologico non è mai stato così rapido. A seguito della digitalizzazione e della conseguente modernizzazione e interconnessione di tutti i sistemi dell'esercito, le competenze in questo settore acquistano un'importanza sempre maggiore e, allo stesso tempo, per l'esercito diventa sempre più impegnativo garantire la pianificazione, l'acquisto e l'esercizio di tali mezzi. Questo anche perché le tecnologie sono, da un lato, uno dei fattori chiave nella configurazione degli eserciti moderni e, dall'altro, un elemento indispensabile per la buona riuscita degli impieghi. La scelta delle tecnologie adeguate è quindi fondamentale. I sistemi militari devono continuare a essere gestibili anche per un esercito di milizia. Nell'ambito della pianificazione, dell'acquisto e dell'esercizio dei propri mezzi d'impiego, per l'esercito è indispensabile disporre delle competenze tecnico-scientifiche necessarie per valutare i rischi in termini di costi, benefici e vulnerabilità delle tecnologie utilizzate.

Dopo il 2017 – anno della presentazione del postulato – sono stati emanati i Principi del Consiglio federale in materia di politica d'armamento del DDPS, incentrati sull'obiettivo di assicurare competenze tecnologiche e capacità industriali. L'Aggruppamento Difesa e l'Ufficio federale dell'armamento (armasuisse) hanno già adottato diverse misure volte a raggiungere tale obiettivo, tra cui l'introduzione del corso di formazione Cyber, della *ICT Warrior Academy*, del *Cyber-Defence Campus* e dell'attribuzione differenziata dei militari in occasione del reclutamento. L'Aggruppamento Difesa e armasuisse analizzano ed elaborano costantemente i vari aspetti della trasformazione digitale, li integrano nei documenti di base strategica e concretizzano in modo graduale le corrispondenti misure.

2 Mandato

Il 14 marzo 2017 il consigliere nazionale Marcel Dobler ha presentato il postulato 17.3106 *Esercito 2.0. La Svizzera deve promuovere e garantire il know-how tecnologico*, con il seguente testo:

Il Consiglio federale è incaricato di verificare come l'esercito intenda soddisfare a lungo termine il crescente fabbisogno di competenze nel settore delle nuove tecnologie. Dovrà tener conto in particolare dei seguenti aspetti:

1. *Come soddisfare a livello di personale il fabbisogno di competenze in continua crescita nel settore tecnologico e scientifico.*
2. *Verifica del fabbisogno di collaboratori in ambito scientifico e tecnologico per l'esercito attuale e futuro, ad esempio per far fronte alle sfide sempre maggiori in ambito cyber e allo sviluppo tecnologico.*
3. *Collaborazione con gli istituti formativi e il mondo economico (comprese le aziende federali, sull'esempio di Israele).*
4. *Il ruolo dei militari: possibilità di militari in ferma continuata con competenze in ambito scientifico; impieghi più lunghi; periodi di pratica in ambito scientifico e tesi di dottorato computabili come giorni di servizio.*
5. *Nuovi criteri per la valutazione dell'idoneità al servizio per chi vanta conoscenze specialistiche (idoneità differenziata); nuovi meccanismi di promozione per gli specialisti che devono rimanere più a lungo nel sistema.*

Nel postulato il crescente fabbisogno è motivato dal fatto che i sistemi autonomi, la protezione dagli attacchi nello cyberspazio, la gestione delle informazioni e la necessità di garantire servizi di comunicazione solidi assumono un ruolo sempre più importante. Anche l'esercito deve occuparsi di questa evoluzione e del passaggio dall'hardware al software. Va inoltre promossa la collaborazione con le istituzioni scolastiche e il mondo economico per costruire e mantenere a lungo termine un know-how fondamentale.

Il Consiglio nazionale ha accolto il postulato il 16 giugno 2017.

3 Competenze tecnologiche

A seconda della natura del compito (pianificazione delle forze armate e dell'armamento, impiego, esercizio e manutenzione di sistemi, istruzione), per soddisfare le esigenze dell'esercito sono necessarie diverse forme e diversi gradi di know-how tecnologico. Occorre inoltre tenere conto di diversi settori rilevanti, che sono esposti qui di seguito.

3.1 Amministrazione

L'importanza delle nuove tecnologie e il conseguente fabbisogno di know-how tecnologico rappresentano una sfida non solo per l'esercito, ma anche per l'Amministrazione. Per questo vengono costantemente esaminate possibili soluzioni per sviluppare o mettere a disposizione le necessarie competenze tecnico-scientifiche. Nella Strategia nazionale del 18 aprile 2018 per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018–2022 il Consiglio federale ha stabilito che lo sviluppo delle competenze e delle conoscenze è alla base dell'uso delle nuove tecnologie. Ciò deve essere garantito, in particolare, mediante l'individuazione precoce di tendenze e tecnologie, lo sviluppo di conoscenze nonché l'ampliamento e la promozione delle competenze di ricerca e formazione. I Principi del Consiglio federale del 24 ottobre 2018 in materia di politica d'armamento del DDPS riprendono questi aspetti e si concentrano sul fabbisogno di competenze tecnologiche e di capacità industriali¹ nonché sulle varie modalità con cui la Svizzera può soddisfare tale fabbisogno.

Il know-how necessario nell'ambito della sicurezza viene sviluppato in collaborazione con partner provenienti da centri di competenza interni ed esterni, da organizzazioni di sicurezza nazionali e internazionali, dal mondo scientifico e dall'industria. In questo contesto, la Confederazione (armasuisse, UFPP e DFAE/DP) conduce ricerche nell'ambito pubblico secondo l'articolo 16 capoverso 1 della legge federale del 14 dicembre 2012² sulla promozione della ricerca e dell'innovazione (LPRI), in particolare nel settore «politica di sicurezza e di pace». La ricerca di armasuisse ha l'obiettivo di assicurare a lungo termine le necessarie conoscenze specialistiche e le competenze tecnico-scientifiche fondamentali affinché l'esercito e altri strumenti della politica di sicurezza possano disporre delle capacità richieste³.

Nel quadro dello sviluppo delle forze armate e della pianificazione dell'armamento, l'Aggruppamento Difesa individua per ogni ambito le tendenze significative in atto. Tra queste figura anche la tecnologia, che è uno dei principali fattori trainanti⁴. In tale ambito, armasuisse garantisce le necessarie competenze tecnico-scientifiche sia per l'esercito che per il DDPS e, con il proprio settore di competenza Scienza e tecnologia (S+T), che costituisce il polo tecnologico del DDPS, è anche responsabile delle attività nel campo della ricerca orientata all'applicazione. Basandosi su una gestione integrale della tecnologia, armasuisse S+T assegna mandati di ricerca nel quadro di programmi di

¹ Secondo i [Principi del Consiglio federale in materia di politica d'armamento del DDPS](#), la politica d'armamento serve a garantire che l'esercito e altre istituzioni statali incaricate della sicurezza della Confederazione siano dotate, tempestivamente, secondo principi economici e in modo trasparente, dell'equipaggiamento, dell'armamento e delle prestazioni necessari. È incentrata in particolare sul fabbisogno dell'esercito di conoscenze specialistiche critiche, tecnologie chiave per la sicurezza, nonché sistemi, beni, costruzioni e servizi tecnologicamente complessi; sono di particolare importanza anche la salvaguardia delle competenze fondamentali e delle capacità industriali volte a garantire l'esercizio affidabile, la capacità d'impiego e la capacità di resistenza dei sistemi dell'esercito.

² RS 420.1

³ I piani di ricerca dell'UFPP, di armasuisse e del DFAE/DP vengono raggruppati come [ricerca del settore pubblico nell'ambito della politica di sicurezza e di pace](#) (link in tedesco e in francese) e coordinati dalla Segreteria di Stato per la formazione, la ricerca e l'innovazione (SEFRI) con i programmi pluriennali di altri settori politici.

⁴ Il piano direttore per l'attuazione della Strategia TIC della Confederazione 2020–2030 contiene, tra le altre cose, iniziative strategiche per sostenere l'attuazione della trasformazione digitale.

ricerca⁵ orientati, dal punto di vista contenutistico, al fabbisogno dell'esercito e utilizza a tal fine le reti consolidate con le università, le scuole universitarie, gli istituti, l'industria e l'Amministrazione in Svizzera e all'estero.

Spazi per l'innovazione

Come strumento supplementare, sono attualmente in fase di creazione all'interno del DDPS i cosiddetti spazi per l'innovazione, volti a consentire una migliore gestione dei continui cambiamenti del contesto globale dovuti soprattutto ai cicli di prodotto sempre più brevi. Uno spazio per l'innovazione consiste in un gruppo di lavoro temporaneo specificamente dedicato a un determinato tema e composto dal servizio richiedente e dal servizio d'acquisto nonché da altri servizi competenti, eventualmente anche esterni. In questo modo è ad esempio possibile individuare le lacune nelle competenze tecnologiche e sviluppare le conoscenze necessarie.

Trasformazione della Base d'aiuto alla condotta (BAC) in un Comando Cyber

Tenendo conto dell'attuale situazione di minaccia, il Consiglio federale vuole trasformare la BAC in un Comando Cyber a partire dal 2024. La modernizzazione di tutti i sistemi dell'amministrazione militare e dell'esercito richiede un'architettura informatica uniforme di livello elevato e l'utilizzo di applicazioni TIC standardizzate. Di pari passo con la sempre maggiore interconnessione aumentano inoltre notevolmente le sfide nell'ambito della cyber-protezione. Per poter rispondere in modo più adeguato a tali esigenze in futuro, occorre trasformare la BAC da ampia organizzazione d'appoggio in un Comando militare orientato all'impiego. Il futuro Comando Cyber dovrà fornire le capacità militari chiave negli ambiti «quadro della situazione», «cyber-difesa», «prestazioni TIC», «aiuto alla condotta», «crittologia» e «guerra elettronica».

Per quanto riguarda il personale, l'amministrazione militare è in concorrenza con il mercato del lavoro civile e risente direttamente della carenza di personale informatico specializzato. A causa della particolarità del loro lavoro, i nuovi collaboratori dell'amministrazione militare richiedono spesso un'ampia formazione continua. Selezionando un candidato tra le formazioni della milizia informatica, questo sforzo può essere solo parzialmente ridotto. La necessità di riunire le competenze e le prestazioni in un comando costituisce un vantaggio per l'acquisizione e la formazione di collaboratori qualificati.

3.2 Base tecnologica e industriale rilevante in materia di sicurezza

Il know-how tecnologico necessario per la sicurezza della Svizzera non può essere sviluppato soltanto all'interno dell'Amministrazione e dell'esercito. È fondamentale anche rafforzare la base tecnologica e industriale rilevante in materia di sicurezza (STIB), che deve essere in grado di garantire la disponibilità delle competenze tecnologiche e delle capacità industriali prioritarie con il necessario know-how in Svizzera. A tal fine, secondo i Principi del Consiglio federale in materia di politica d'armamento del DDPS, la Confederazione dispone di sette strumenti di gestione⁶.

Sulla base del fabbisogno dell'esercito, armasuisse S+T ha definito le tecnologie che rivestono un'importanza fondamentale per la Svizzera. Queste cosiddette tecnologie chiave per la sicurezza –

⁵ I programmi di ricerca sono i seguenti: 1) Ricognizione e sorveglianza, 2) Tecnologia della comunicazione, 3) Cyberspazio e informazione, 4) Efficacia bellica, protezione e sicurezza, 5) Sistemi mobili senza pilota e 6) Individuazione tempestiva degli sviluppi tecnologici.

⁶ Gli strumenti di gestione per il rafforzamento della STIB sono i seguenti: 1) acquisti in Svizzera, 2) affari offset, 3) cooperazione internazionale, 4) ricerca applicata, 5) promozione dell'innovazione, 6) scambio di informazioni con l'industria e 7) politica dei controlli delle esportazioni.

come ad esempio le tecnologie della comunicazione, dell'informazione e dei sensori – sono mantenute in Svizzera e rafforzate mediante una gestione mirata da parte della Confederazione. Inoltre, vengono periodicamente adeguate in funzione dello sviluppo tecnologico e del fabbisogno dell'esercito.

La STIB deve fornire prestazioni fondamentali affinché l'industria possa sostenere i sistemi d'impiego dell'esercito con l'affidabilità e la capacità di resistenza necessarie. Per farlo servono capacità volte a garantire la gestione e la manutenzione dei sistemi militari attuali e futuri. Allo stesso tempo, sono necessarie capacità specifiche per consentire ad esempio l'integrazione di nuove componenti nei sistemi militari nel quadro delle misure di mantenimento del valore. Dalla STIB ci si aspetta inoltre la capacità di sviluppare e produrre componenti di importanza critica cruciali ai fini della sicurezza.

3.3 Personale dell'esercito

Il sistema di milizia è molto importante per l'esercito, poiché rende possibile uno scambio di conoscenze e competenze provenienti dai settori più disparati. Utilizzate in modo mirato, permette infatti a entrambe le parti di sfruttare efficacemente le competenze civili durante i corsi di ripetizione o il servizio in ferma continuata. Ciò vale anche per le tecnologie moderne: sia nell'ambito del reclutamento sia durante il periodo del servizio, grazie al sistema di milizia è possibile acquisire in maniera mirata un numero crescente di specialisti con le competenze tecnologiche e scientifiche necessarie, impiegandoli poi nel rispettivo ambito specialistico affinché l'esercito possa approfittare del loro bagaglio di conoscenze civili. In questo contesto occorre porre l'accento sul fatto che i vantaggi sono reciproci, vale a dire che a loro volta i militari possono trarre profitto dal loro servizio anche per la vita civile.

Corso di formazione cyber

L'esercito organizza il corso di formazione cyber due volte all'anno e a ogni corso partecipano circa una dozzina di specialisti in ambito informatico (IT). Il corso di formazione dura 40 settimane e prevede 800 ore d'istruzione suddivise nei seguenti moduli: «Basi generali», «Basi tecniche», «Istruzione trasversale» (armonizzazione delle conoscenze), «Formazione alla condotta», «Istruzione specialistica» nonché «Impiego ed esercizi». Al fine di raggiungere gli impegnativi obiettivi didattici, durante il corso di formazione vengono combinati svariati metodi d'insegnamento (ad es. insegnamento diretto, elaborazione autonoma dei contenuti o applicazione e approfondimento delle conoscenze acquisite). Per garantire che la materia insegnata sia sempre attuale e affinché sia possibile mantenere i contatti con le istituzioni scolastiche in Svizzera, vengono impiegati sia docenti della BAC sia insegnanti esterni.

La promozione a sergente prevista durante il corso di formazione cyber consente alle persone che concludono con successo il corso per ottenere un grado superiore e, pertanto, di rimanere più a lungo al servizio dell'esercito mettendo a disposizione le loro conoscenze specifiche. Inoltre, dall'autunno del 2019, chi conclude con successo il corso di formazione cyber può assolvere l'esame di *Cyber Security Specialist* con attestato professionale federale.

Per accrescere ulteriormente la qualità dell'istruzione nel quadro del corso di formazione cyber e attuare i requisiti della SNPC (Strategia Nazionale per la Protezione della Svizzera contro i rischi Cyber), l'istruzione in seno all'esercito sarà integrata da uno stage in cooperazione con partner esterni. In questo modo è possibile approfondire e ampliare le capacità apprese e successivamente farne beneficiare l'esercito. I partner per lo svolgimento dello stage sono di preferenza autorità cantonali, gestori delle infrastrutture critiche e imprese svizzere che operano nel settore IT/cyber. Il primo concetto è stato verificato in un progetto pilota nell'estate del 2019. I riscontri degli offerenti di stage esterni nell'ambito del test pilota confermano l'elevata qualità dell'istruzione di base e dell'istruzione specialistica nel corso

di formazione cyber. In questo modo l'esercito contribuisce attivamente a uno scambio e all'aumento della qualità dell'istruzione nel settore cyber.

Attribuzione differenziata

Grazie all'attribuzione differenziata, ormai da due anni è possibile incorporare nella truppa anche persone soggette all'obbligo di leva che presentano limitazioni delle capacità fisiche, ad esempio per quanto riguarda la capacità di portare o sollevare pesi o di marciare. Questo aspetto verrà considerato anche nella revisione delle direttive in materia di idoneità al servizio (regolamento *Nosologia Militaris*). La competenza per la valutazione di persone soggette all'obbligo di leva e militari con notevoli limitazioni fisiche spetta ad apposite commissioni per la visita sanitaria. Queste esaminano individualmente – senza pregiudizio per altri casi – l'idoneità a svolgere la funzione militare specifica prevista. In questo modo si garantisce che gli specialisti possano prestare servizio militare anche con limitazioni fisiche, sempre che ciò sia giustificabile dal punto di vista medico. L'obiettivo primario nella valutazione dell'idoneità al servizio è e rimane quello di garantire che, con il servizio previsto, le persone dichiarate idonee al servizio militare non pregiudichino né la loro salute né quella dei loro camerati.

Apporto di personale

La soluzione più duratura per mantenere più a lungo il know-how specifico all'interno del sistema dell'esercito è la promozione, con la quale si prolunga il numero massimo di giorni di servizio da prestare. Per far sì che ad esempio gli specialisti provenienti dall'industria rimangano più a lungo nell'esercito, si può ricorrere al sistema di promozione degli ufficiali specialisti⁷ (240 giorni di servizio d'istruzione a partire dalla nomina). Inoltre, per tutti i gradi è possibile procedere a una nomina a specialista in base alla funzione. Anche con questa procedura, il militare in questione presta giorni di servizio supplementari. All'occorrenza e su domanda congiunta della persona interessata e del comando competente, l'esercito può prorogare l'obbligo di prestare servizio militare per i sottufficiali superiori e gli ufficiali superiori al fine di continuare ad avvalersi delle loro conoscenze.

Il quadro giuridico è costituito dalla legge militare (LM; RS 510.10; art. 42) e dall'ordinanza concernente l'obbligo di prestare servizio militare (OOPSM; RS 512.21; art. 47), in cui è stabilito quanti giorni di servizio d'istruzione computabili devono essere prestati nel servizio militare di milizia. Non appena i militari hanno prestato il numero massimo di giorni di servizio, l'esercito non può più ricorrere al loro know-how. Con la revisione della legge militare attualmente in corso si mira ad aumentare da 280 a 300 il numero massimo di giorni di servizio d'istruzione per i militari in ferma continuata.

Nell'ottica dell'apporto di personale sono stati verificati, armonizzati e all'occorrenza adeguati i profili dei requisiti delle funzioni di reclutamento per la prima incorporazione dei militari a partire dal 1° luglio 2019 ed è stata creata la possibilità di specializzarsi nell'ambito della funzione durante l'istruzione. In questo modo è possibile rivolgersi ai giovani talenti con capacità particolari nel settore delle tecnologie moderne e reclutarli per la funzione militare adeguata già prima che intraprendano la loro formazione specialistica. A ciò si aggiunge la possibilità di procedere a un cambiamento d'incorporazione per i militari incorporati che abbiano svolto una pertinente formazione continua in ambito civile e di impiegargli in funzioni o formazioni adeguate. L'esercito cerca proattivamente potenziali candidati per funzioni informatiche specifiche, ma è anche possibile candidarsi spontaneamente.

Per fare in modo che le conoscenze specialistiche dei militari possano essere sfruttate più a lungo, occorre prendere in esame diversi modelli. Un esempio in tal senso è la (parziale) computabilità delle tesi di master o di dottorato. Ciò avviene già per gli specialisti nonché per gli aspiranti delle funzioni di

⁷ Conformemente all'articolo 80 dell'ordinanza concernente l'obbligo di prestare servizio militare (OOPSM; RS 512.21), le funzioni di ufficiale per le quali le conoscenze altamente specialistiche necessarie per svolgere la funzione sono nettamente preminenti rispetto all'istruzione a ufficiale, possono essere conferite a ufficiali specialisti. Ciò vale in egual misura per tutti i settori di compiti dell'esercito.

medico, dentista o farmacista. Per quanto riguarda le formazioni altamente specialistiche per ufficiali delle funzioni summenzionate, il servizio può essere svolto – in uniforme e sotto un comando militare – interamente o in parte presso un'istituzione civile specializzata, sempre che l'esercito non possa garantire autonomamente la formazione. Tuttavia, per il computo delle formazioni civili è necessaria anche la volontà, da parte dei militari interessati, di mettersi a disposizione per un periodo di tempo più lungo.

Il piano d'azione *Cyber Defence* del DDPS prevede di aumentare notevolmente negli anni a venire gli effettivi di personale nel settore cyber, anche per il personale di milizia. Per il 1° gennaio 2022 è prevista la costituzione di un battaglione e di uno stato maggiore speciale cyber, con conseguente incremento degli effettivi del personale di milizia dai circa 200 militari attuali a 575 militari. Con l'aumento del personale di milizia si migliorerà innanzitutto la capacità di resistenza dei mezzi operativi dell'esercito in ambito cyber. A tal fine, gli specialisti cyber di milizia sono assegnati ai rispettivi reparti dell'esercito.

3.4 Personale professionista militare e civile

Il reclutamento degli specialisti necessari da integrare nel personale professionista militare e civile rappresenta una sfida per l'esercito a causa della situazione sul mercato del lavoro. Il marketing del personale è già stato intensificato, ad esempio esaminando nuove modalità di reclutamento, utilizzando più attivamente i social media o offrendo occupazioni a tempo parziale durante la formazione terziaria, ma occorrerà del tempo prima che queste misure mostrino la loro efficacia. Per questo motivo non è ancora possibile valutarne l'impatto sugli effettivi futuri.

In aggiunta al reclutamento di personale con know-how specifico sul mercato del lavoro, saranno incentivati anche lo sviluppo e l'ampliamento delle competenze dei collaboratori. A tal fine, il DDPS garantisce costantemente che lo sviluppo del personale, dei quadri e delle carriere siano armonizzati tra loro, ampliandoli all'occorrenza. I collaboratori possono ad esempio frequentare corsi del Centro di formazione dell'Amministrazione federale (CFAF) oppure stipulare accordi di formazione individuali nel caso in cui seguano corsi presso un istituto formativo esterno alla Confederazione.

Oltre all'incremento degli effettivi del personale di milizia, il piano d'azione *Cyber Defence* del DDPS prevede di aumentare di circa la metà, negli anni a venire, anche il personale professionista nel settore cyber. A tal fine, il personale dell'amministrazione militare è assegnato, nell'ambito delle sue funzioni professionali, a diverse divisioni all'interno della BAC.

ICT Warrior Academy

Nei settori dell'informatica e delle tecnologie dell'informazione e della comunicazione (TIC), la *ICT Warrior Academy* della BAC è il centro di competenza dell'Aggruppamento Difesa per la formazione e la formazione continua in ambito civile, volte a sviluppare e a mantenere le necessarie capacità dei collaboratori. A tal fine vengono offerti corsi di formazione sia teorici che pratici per determinate funzioni nonché per determinati metodi e tecnologie. La formazione viene sviluppata in collaborazione con scuole universitarie (professionali) e con il coinvolgimento di partner e comprende temi come il *Design Thinking*, la gestione dei servizi informatici, l'ingegneria del software o la cyber-sicurezza. La *ICT Warrior Academy* si rivolge sia ai collaboratori di lunga data sia ai nuovi collaboratori che vengono formati in modo specifico presso la BAC per la funzione prevista.

In tale ambito, il nuovo programma *ICT Warrior School* lavora intensamente sulle prestazioni, competenze e infrastrutture TIC per i prossimi cinque / dieci anni. I professionisti vengono valutati in riferimento alle loro attuali attività e al loro potenziale, invitati a seguire una formazione continua e reimpiegati secondo le loro capacità.

4 Collaborazione con i partner

Il DDPS punta a intensificare sempre di più la collaborazione in seno all'Amministrazione federale, intrattiene partenariati con istituzioni scolastiche e, tramite armasuisse, collabora direttamente con l'industria. Nell'ottica dell'evoluzione tecnologica, il DDPS si adopera costantemente per ampliare le collaborazioni esistenti e per avviare nuovi partenariati.

4.1 Istituti formativi

L'Aggruppamento Difesa e diversi istituti formativi hanno concluso contratti di cooperazione per garantire il reciproco riconoscimento delle formazioni. Con numerosi istituti formativi di livello terziario sono stati conclusi accordi che disciplinano il computo dei contenuti della formazione militare negli studi da assolvere nonché nei periodi di pratica, nella formazione di base, nei cicli di studio consecutivi e nei corsi di formazione continua. I militari possono ad esempio farsi computare i punti ECTS da determinate scuole universitarie se hanno assolto una formazione alla condotta presso l'Istruzione superiore dei quadri dell'esercito. Sono inoltre stati stipulati accordi di formazione in campo tecnico-scientifico, ad esempio con l'Università di Zurigo, il Politecnico federale di Zurigo (PFZ) e la Scuola universitaria professionale di Lucerna.

Cyber-Defence Campus

Il *Cyber-Defence Campus (CYD Campus)* è un centro di competenza cyber creato dal DDPS sotto la guida di armasuisse. Mira a promuovere una ricerca innovativa e orientata all'applicazione nel campo della scienza della sicurezza e dei dati nonché – in collaborazione con start-up e imprese già affermate nel settore della sicurezza – a tradurre in soluzioni i risultati della ricerca. Il suo scopo principale è individuare le tecnologie e le tendenze in ambito cyber e valutarle in termini di benefici. Le conoscenze necessarie vengono sviluppate insieme alle scuole universitarie e all'industria, con il supporto delle tre sedi del *CYD Campus* a Thun (armasuisse), Zurigo (PFZ) e Losanna (Politecnico federale di Losanna [PFL]). L'obiettivo primario del campus è quello di tradurre i risultati della ricerca di base in prototipi e modelli nonché di avviare partenariati.

Cyber-Defence Fellowship

Nel 2020 il *CYD Campus* e il PFL hanno lanciato congiuntamente il programma svizzero per talenti *Cyber-Defence*. L'obiettivo è quello di ampliare la ricerca e l'insegnamento nel campo della cyber-difesa mettendo insieme la ricerca accademica e quella applicata. Da un lato si devono sviluppare soluzioni nei settori della sicurezza delle reti e della scienza dei dati. D'altro canto, i partecipanti dovrebbero occuparsi di questioni scientifiche e tecnologiche che vanno oltre a questi argomenti.

Nel quadro delle *Cyber-Defence Fellowship*, due volte all'anno vengono pubblicati bandi per progetti di ricerca a livello di master, dottorato e post-dottorato. Il programma di *fellowship* (limite di spesa: 1 mio CHF circa all'anno) consente a studenti, dottorandi e post-dottorandi di realizzare i propri lavori o progetti di ricerca presso il *CYD Campus* sotto la supervisione di un docente di un istituto universitario svizzero. Con questo programma di talenti si mira non solo a sviluppare soluzioni tecnologiche e tecniche nel settore della cyber-difesa, ma anche a dar vita a una nuova generazione di esperti in ambito cyber.

Supervisione di lavori scientifici e stage

Nell'ambito di programmi di ricerca, armasuisse commissiona lavori scientifici alle università e alle scuole universitarie professionali svizzere e li supervisiona. In termini concreti, attualmente una cinquantina di tesi di bachelor, master, dottorato e post-dottorato copre un'ampia gamma di questioni tecnologiche importanti per l'esercito. Il limite di spesa è di circa 5 milioni di franchi all'anno.

Questi lavori scientifici possono anche essere elaborati nel quadro del Centro svizzero dei droni e della robotica (CSDR) di armasuisse (in collaborazione con il PFZ). Nel prossimo futuro ci si concentrerà sempre di più anche sul tema dello spazio. Si mira a far sì che gli studenti acquisiscano precocemente familiarità con le questioni tecnologiche di rilevanza militare, suscitando in tal modo il loro interesse per i temi trattati. Le esperienze così maturate potranno poi facilitare il loro ingresso nell'esercito o nei settori tecnologici del DDPS.

Gli studenti possono svolgere presso armasuisse uno stage di durata compresa fra tre mesi e un anno in base all'ordinamento degli studi delle rispettive università o scuole universitarie professionali. Inoltre, armasuisse offre l'opportunità di svolgere stage individuali, ad esempio per facilitare la scelta dell'indirizzo di studio. Questi stage consentono ad armasuisse di individuare precocemente potenziali talenti e di farsi conoscere come possibile datore di lavoro.

4.2 Economia privata

La collaborazione con l'economia privata in Svizzera e all'estero è descritta nei Principi del Consiglio federale in materia di politica d'armamento del DDPS, come anche la summenzionata rilevanza della STIB o il ruolo della RUAG. Nell'ambito dello scorporo della RUAG Holding SA, le divisioni che lavorano per l'esercito sono state separate dal resto della RUAG e riunite in una nuova società autonoma del gruppo, che di regola fornisce prestazioni unicamente a favore dei sistemi dell'esercito. La nuova società autonoma del gruppo diventa inoltre, in linea di principio, il centro di competenza per il materiale nel quadro dell'acquisto di sistemi complessi e importanti ai fini della sicurezza.

La collaborazione diretta con l'industria nel settore dell'innovazione rappresenta una sfida. Il DDPS ha adottato misure per ottimizzare l'iter degli acquisti, anche in considerazione della crescente importanza delle collaborazioni con l'industria nel contesto della rapida evoluzione tecnologica.

4.3 Cooperazione internazionale

Lo sviluppo tecnologico svolge un ruolo importante anche nella cooperazione dell'Aggruppamento Difesa e di armasuisse con altri Stati e organizzazioni internazionali. Le cooperazioni internazionali servono, tra le altre cose, a garantire e a mantenere l'accesso a capacità, know-how e competenze all'estero.

L'accento è posto sulla cooperazione con gli Stati limitrofi, con Stati e organizzazioni internazionali nello spazio europeo nonché con leader tecnologici globali. Attraverso contatti regolari vengono ad esempio analizzate le sfide legate alla trasformazione digitale nell'ambito di formazioni ed esercitazioni congiunte nonché mediante lo scambio reciproco di esperienze. Le cooperazioni internazionali offrono inoltre piattaforme per progetti di ricerca comuni. Ciò è particolarmente importante per la Svizzera nel caso in cui in specifici settori di ricerca manchino di competenze o infrastrutture proprie.

Un esempio di tale collaborazione è la partecipazione della Svizzera al Centro di eccellenza per la cyber-difesa cooperativa (CCD COE) di Tallinn (in Estonia), che incentiva la cooperazione internazionale nell'ambito della ricerca e della formazione in materia di cyber-difesa e cyber-sicurezza. Questa cooperazione consente alla Svizzera di accedere alle conoscenze e alle informazioni, oltre che

alle diverse attività del CCD COE, sia nell'ambito della ricerca che della formazione. Tale partecipazione contribuisce all'attuazione della SNPC. Inoltre, nel quadro di questa cooperazione, la Svizzera potrà inviare a Tallinn uno o due specialisti civili o militari.

5 Conclusione

Lo sviluppo tecnologico e la conseguente trasformazione digitale si ripercuotono anche sul DDPS e sull'esercito. Per fare in modo che in futuro sia l'esercito che l'Aggruppamento Difesa dispongano di un numero sufficiente di specialisti con competenze tecnologiche e scientifiche, sono state avviate o già attuate diverse misure.

Per quanto concerne i militari di milizia, oltre al sistema di promozione degli ufficiali specialisti e alla nomina a specialista in base alla funzione c'è anche la possibilità di procedere a un cambiamento d'incorporazione per i militari incorporati che abbiano svolto una pertinente formazione continua in ambito civile, ad esempio nel settore informatico, e di impiegarli in funzioni o formazioni adeguate. Grazie all'attribuzione differenziata è anche possibile reclutare un maggior numero di persone soggette all'obbligo di leva per lo svolgimento di una formazione in seno all'esercito. Inoltre, il nuovo corso di formazione cyber si rivolge direttamente ai militari con conoscenze specifiche nel settore informatico. Infine, il riconoscimento da parte di istituti formativi civili rende più interessanti determinate formazioni in ambito militare.

Per quanto riguarda il personale professionista, oltre che sul reclutamento ci si concentra anche sulla formazione e sulla formazione continua a livello interno, ad esempio mediante la *ICT Warrior Academy* presso la BAC. Inoltre, in collaborazione con università e scuole universitarie professionali viene offerta la supervisione di lavori scientifici, stage e programmi di ricerca. L'obiettivo è individuare precocemente e promuovere i talenti nonché facilitare ai futuri esperti specializzati l'ingresso nell'amministrazione militare.

Per far sì che il know-how tecnologico possa essere sviluppato e mantenuto, viene promossa la collaborazione all'interno dell'Amministrazione e con partner in Svizzera e all'estero. A tal fine vengono stipulati accordi di formazione con istituzioni scolastiche o sviluppati programmi di talenti come le *Cyber-Defence Fellowship*. Inoltre, sotto la guida di armasuisse, il DDPS ha creato un *CYD Campus* che, tra le altre cose, in collaborazione con start-up e imprese già affermate nel settore della sicurezza traduce in soluzioni i risultati della ricerca. Conformemente ai Principi del Consiglio Federale in materia di politica d'armamento del DDPS, anche l'economia privata viene coinvolta nel settore delle tecnologie chiave per la sicurezza. Con queste misure si mira ad acquisire la più ampia gamma possibile di conoscenze e capacità a beneficio dell'esercito.

La tecnologia, la collaborazione con i partner e il personale adeguatamente formato svolgeranno in futuro un ruolo ancora più importante di quello che ricoprono oggi. Per questo motivo il DDPS considera e promuove ulteriormente i partenariati esistenti, ne avvia di nuovi, si impegna a favore della ricerca e dello sviluppo e si adopera per l'acquisizione duratura e a lungo termine di personale (di milizia) con know-how tecnologico.