Rapporto di attività 2024

dell'Autorità di vigilanza indipendente sulle attività informative (AVI-AIn)

1 Sintesi

Come già nell'anno precedente, la situazione in materia di sicurezza non solo non è migliorata, ma si è ulteriormente aggravata. Ciò ha comportato, in alcuni casi, nuove sfide per i servizi di intelligence soggetti alla vigilanza dell'Autorità di vigilanza indipendente sulle attività informative (AVI-AIn) come pure la necessità, da parte di quest'ultima, di adeguarsi in modo flessibile alle nuove circostanze nell'ambito della propria attività di verifica e di rivedere in parte le sue priorità.

La necessità di trasformare i servizi a seguito del cambiamento della situazione ha richiesto un notevole impegno da parte dell'AVI-AIn. Non è solo il Servizio delle attività informative della Confederazione (SIC) a trovarsi in una fase di trasformazione, ma anche il Servizio delle attività ciber ed elettromagnetiche (ACE), che dal 2024 svolge le proprie attività di intelligence nel quadro del Comando Ciber. Nel Servizio informazioni militare (SIM) è previsto un ampliamento del Servizio di protezione preventiva dell'esercito (SPPEs). Alla luce del mandato conferito all'SPPEs dal SIC, ciò ha sollevato per l'AVI-AIn la questione di definire l'ampiezza delle proprie competenze e dei propri obblighi di controllo su tali attività nell'ambito del proprio mandato legale.

Gli sviluppi tecnologici che possono essere sfruttati per le attività di intelligence devono essere non solo osservati, ma anche compresi dalle autorità di vigilanza. Per questo motivo, anche nel 2024 si è investito nella formazione del personale, sia attraverso la partecipazione a congressi su temi tecnici di attualità sia mediante specifiche formazioni continue. Come emerge dagli scambi con altre autorità di vigilanza a livello internazionale, l'AVI-AIn non è l'unica a dover affrontare notevoli sfide a causa degli sviluppi tecnologici e della conseguente necessità di adattarsi alle mutevoli condizioni quadro.

Non sono state svolte – e concluse – verifiche solo presso il SIC. Una verifica ha riguardato anche l'ACE, mentre un'altra ha coinvolto il SIM. In relazione al SIM, l'AVI-AIn ha proseguito i colloqui iniziati nel 2023 a livello di direzione in merito alle sue competenze in materia di vigilanza nel settore dell'SPPEs. La corrispondente verifica prevista nel piano di controllo 2024 non era ancora stata avviata al momento della chiusura redazionale del presente rapporto.

2 Indice

3 Cifre al 31 dicembre 2024

Collaboratori	01.01.2024	**9**
	31.12.2024	**9**
Verifiche in corso al 01.01.2024		**10**
Verifiche avviate nel 2024		**9**
Verifiche concluse nel 2024		**11**
Verifiche in corso al 31.12.2024		**9**
Verifiche pianificate		**10**
Verifiche non pianificate		**1**
Raccomandazioni		**14**

4 Nota personale

A cosa servono i controlli?

Ogni attività persegue un obiettivo. In alcuni ambiti, l'obiettivo si raggiunge con un risultato tangibile, come un prodotto, un servizio. In altri ambiti questo non è possibile, come le attività di prevenzione per la sicurezza nazionale. Difatti, un attentato sventato non è un risultato tangibile. Addirittura, a volte non è nemmeno possibile sapere se il temuto attentato non ha avuto luogo perché la prevenzione è stata efficace o perché l'attentatore ha avuto un attacco di febbre. Come sempre nella vita, ci vuole anche un po' di fortuna.

Anche i controlli, generalmente, sono un'attività di prevenzione che non si traduce facilmente in constatazioni tangibili, quanto piuttosto in un miglioramento del sistema.

Nel nostro caso, quale autorità di sorveglianza sulle attività informative, ci confrontiamo con la duplice sfida di rendere la nostra attività "tangibile" per la popolazione, ma prima ancora di provocare miglioramenti "tangibili" presso i servizi sorvegliati. Ci siamo riusciti? Il nostro rapporto sulle attività di sorveglianza 2024 vuole rispondere con sincerità a questa domanda.

Prima di tutto, abbiamo più volte dovuto ribadire la necessità per il Servizio informazioni della Confederazione di rafforzare le proprie competenze giuridiche e gestionali, per garantire al proprio personale un quadro di lavoro competente e sano. Se da un lato il fatto di aver sollevato in più ambiti questo tema è un segno che la prima volta non è bastata, dall'altro lato s'intravvedono ora i segni di una maggior consapevolezza e alcuni sviluppi organizzativi che vanno nella giusta direzione.

Presso il Servizio delle attività informative dell'esercito abbiamo constatato che la gestione dei rischi, come per esempio nel caso di situazioni critiche nuove, funziona in modo pragmatico nel lavoro quotidiano dei collaboratori, ma non trova ancora una consolidazione approvata a livello di processo amministrativo, poiché alcuni aspetti sulla documentazione del processo subiscono una revisione che non è ancora completata. Seguiamo dunque attentamente questo punto, onde assicurarci che la gestione del Servizio rimanga connessa con la sana realtà vissuta dai propri collaboratori.

I controlli servono a volte anche a segnalare che un ambito o un tema su cui noi stiamo intervenendo deve essere sistemato prima di altri, o sistemato e basta. Difatti non interveniamo mai a caso, ma facciamo delle verifiche in base un'analisi dei rischi attuali o ricorrenti. I servizi sorvegliati, inoltre, reagiscono anche migliorando certe situazioni proprio in vista di una verifica.

Vi presentiamo in questo rapporto il riassunto di tutte le nostre verifiche, ma non solo. I nostri riassunti sono ora accompagnati da alcune indicazioni schematiche complementari, per mostrare quali sono le tappe del nostro lavoro, in che tempi e con quanti contatti presso i servizi tiriamo le nostre conclusioni.

In conclusione: a cosa servono i controlli? Servono ad accelerare un'evoluzione positiva, a interrompere una situazione negativa, a correggere un errore, a migliorare un processo lavorativo. Servono ad affidarsi di più a un lavoro svolto professionalmente che alla fortuna.

Vi auguro una buona lettura!

Prisca Fischer, Capo AVI-Aln

5 Attività di vigilanza

5.1 Piano di controllo

L'AVI-AIn svolge verifiche in base a una propria valutazione dei rischi nei seguenti ambiti:

- strategia e pianificazione
- organizzazione e mandati
- collaborazione
- acquisizione
- risorse
- trattamento dei dati e archiviazione

Il piano di controllo è programmato in modo tale che vi sia almeno una verifica per ogni ambito.

5.2 Verifiche nel 2024

Il rapporto di attività dell'AVI-AIn continua a evolversi e contiene pertanto alcune novità:

- le sintesi delle verifiche concluse al 31 dicembre 2024 (fa fede la data della conferma di ricezione o della lettera di attuazione del capo del Dipartimento federale della difesa, della protezione della popolazione e dello sport [DDPS]) sono pubblicate nel rapporto di attività. Per le verifiche in corso, viene pubblicato l'obiettivo della verifica;
- ogni verifica è accompagnata da una tabella introduttiva con quattro informazioni di carattere temporale: la data di inizio della verifica (mandato), la data di invio della bozza del rapporto per il parere dei servizi (consultazione), la data del rapporto definitivo e la data della conferma di ricezione o della lettera di attuazione. Questa tabella fornisce indicazioni sulla durata della verifica e, per le verifiche in corso, sulla fase in cui si trovano attualmente. Infine, viene indicato il numero di interviste (orali o scritte) che sono state svolte fino al 31 dicembre 2024.

5.2.1 Strategia e pianificazione

Nell'ambito «Strategia e pianificazione» l'AVI-AIn svolge verifiche su temi che riguardano la pianificazione strategica a breve, medio o lungo termine delle autorità di intelligence della Svizzera nonché la definizione dei loro obiettivi. Nel 2024 l'AVI-AIn si è occupata della seguente verifica:

24-1 Intelligenza artificiale (IA) presso il SIC

L'AVI-AIn verifica, dal punto di vista della legalità, dell'efficacia e dell'adeguatezza, se il SIC acquisisce, utilizza e controlla correttamente questa tecnologia. Per la verifica in questione sono stati eseguiti lavori preparatori e la verifica avrà luogo nel 2025.

5.2.2 Organizzazione e mandati

Nell'ambito «Organizzazione e mandati», l'AVI-AIn verifica l'idoneità della struttura e dei processi dei servizi informazioni, chiedendosi se possano consentire un adempimento conforme alla legge, adeguato ed efficace del mandato legale di queste autorità. Nel 2024 l'AVI-AIn ha svolto le seguenti verifiche in questo ambito:

23-2 Servizi giuridici nel SIC

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
10.08.2023	15.05.2024	05.08.2024	25.09.2024	40

L'osservanza del principio di legalità e dell'azione conforme alla legge è particolarmente importante nelle attività di intelligence. Da un lato, se il SIC o il suo personale non agiscono in modo conforme alla legge, possono essere violati diversi diritti fondamentali (protezione dei dati, diritto alla protezione della sfera privata, segreto d'affari ecc.); dall'altro, se il SIC non sfrutta appieno le possibilità che la legge gli concede, ne deriva un rischio rilevante per la sicurezza della Svizzera. Inoltre, può sorgere un danno di reputazione, compromettendo la fiducia della popolazione svizzera in questa istituzione. Pertanto,

l’AVI-AIn ha verificato l’adeguatezza e l’efficacia di compiti, competenze e responsabilità dei fornitori di servizi giuridici in seno al SIC.

L’AVI-AIn ha intervistato collaboratori di diversi settori e funzioni in merito a cinque questioni da verificare, ha esaminato i documenti e ha stabilito che, sebbene il SIC adempia il mandato di formazione conferitogli dalla legge, dopo la trasformazione è opportuno ottimizzare l’esecuzione del concetto di formazione per tutti i settori del SIC. Come altre unità amministrative, anche il SIC ha la possibilità di acquisire all’esterno il know-how giuridico mancante. Negli ultimi anni ha conferito solo mandati mirati e motivati per la fornitura di servizi giuridici, senza che ciò indicasse una carenza di risorse specialistiche necessarie.

Sono soprattutto le unità organizzative responsabili del controllo della qualità e della compliance nonché il servizio giuridico del SIC a fornire prestazioni giuridiche. In tutti e tre i settori è stata riscontrata una necessità d’intervento o, perlomeno, sono emerse questioni che richiedono una maggiore attenzione nell’ambito della trasformazione in corso.

Le due raccomandazioni formulate riguardavano le attività dell’unità organizzativa responsabile della compliance e la loro tracciabilità nonché il coinvolgimento attivo del servizio giuridico in determinati affari e l’impostazione dei processi di lavoro. È stata osservata una discrepanza tra le richieste e le aspettative nei confronti del servizio giuridico da un lato e la sua precedente impostazione e competenza decisionale dall’altro. Per fare in modo che la situazione reale corrisponda a quella auspicata non basta aggiornare solo la descrizione della funzione direttiva all’interno del servizio giuridico. Gli ultimi audit di compliance secondo il relativo concetto sono stati effettuati nel 2021. Al momento della verifica, solo il servizio di notifica era gestito attivamente dall’unità organizzativa responsabile della compliance, ma non erano disponibili prove di tale attività. Per quanto riguarda l’unità organizzativa responsabile del controllo della qualità, si sono registrate numerose partenze di personale con formazione giuridica, che deve essere sostituito nel più breve tempo possibile per poter gestire le pendenze nell’aggiornamento della documentazione.

23-4 IT Service Continuity Management (ITSCM) e Disaster Recovery IT nel SIC

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
13.02.2023	11.01.2024	06.02.2024	06.04.2024	4

Nell’ambito di questa verifica, l’AVI-AIn ha esaminato se il SIC dispone di processi efficaci e adeguati per continuare a garantire, in uno scenario di crisi o catastrofe, il funzionamento del suo sistema informatico, e dunque il proseguimento della sua attività principale, e per ripristinare i suoi dati.

Eventi imprevisti importanti, quali incendi, inondazioni o attività criminali, rappresentano una minaccia per qualsiasi organizzazione. Questo tipo di eventi può causare potenzialmente danni più gravi di un semplice guasto, in particolare all’infrastruttura delle tecnologie dell’informazione. Pertanto, le organizzazioni devono preoccuparsi di garantire la continuità della loro attività (Business Continuity Management [BCM]). Il BCM si concentra su un evento e mira a ridurre l’impatto in termini di rischi sulle prestazioni e sui processi operativi critici.

Un sistema informatico affidabile e sempre disponibile è indispensabile per la sopravvivenza di un’impresa la cui attività principale è fortemente dipendente dalle tecnologie dell’informazione. L’IT Service Continuity Management (ITSCM), associato al BCM, ha lo scopo di garantire la fornitura delle prestazioni informatiche critiche identificate dall’impresa in conformità alle esigenze anche in caso di eventi importanti. A tal fine, si valutano e si mettono in atto misure preventive (rafforzamento della resilienza) e misure predisposte in caso di evento (rafforzamento della risposta). L’ITSCM deve garantire che i servizi e l’infrastruttura delle tecnologie dell’informazione e della comunicazione (TIC) siano disponibili dopo un’interruzione o che possano essere ripristinati entro un termine stabilito. Il disaster recovery dell’infrastruttura informatica (Disaster Recovery-IT) invece ha l’obiettivo di ripristinare i servizi e l’infrastruttura TIC dopo un’interruzione.

Un simile ITSCM deve rispondere a rischi attuali e concreti. Con la digitalizzazione che avanza e vista l'importanza centrale del trattamento dei dati nelle attività del SIC, quest'ultimo dipende sempre più dal funzionamento continuo e affidabile delle sue infrastrutture informatiche, il tutto in un contesto caratterizzato dal rischio di penuria di energia elettrica, dal moltiplicarsi dei ciberattacchi e da una guerra sul continente europeo. Inoltre, eventuali perdite di dati rischierebbero di compromettere la capacità del SIC di adempiere il proprio mandato.

Il BCM era già stato oggetto di un rapporto della Revisione interna DDPS (rapporto I 2022-01 del 15 agosto 2022), che conteneva una raccomandazione in cui si invitavano le unità amministrative del dipartimento ad aggiornare la propria documentazione su questo tema. Il SIC si adopera per attuare tale raccomandazione. Inoltre, la direzione del SIC ha deciso di approvare e attuare un nuovo BCM soltanto dopo che sarà stata ultimata la trasformazione attualmente in corso. L'AVI-AIn non ha quindi insistito ulteriormente per quanto riguarda il BCM.

Quanto all'ITSCM, l'AVI-AIn ha riscontrato lacune nella documentazione dovute a un errore di governance IT all'interno del SIC. Quest'ultimo ha preso provvedimenti, ma solo a livello tecnico. L'unità TIC del SIC ha invece adottato numerose misure volte a garantire la continuità dell'attività in caso di evento importante. Le misure adottate – tra cui in particolare la ridondanza dell'infrastruttura TIC e la strategia di salvataggio dei dati – sono efficaci e adeguate e permettono di ridurre al minimo i rischi in modo coerente. Tuttavia, non è stata messa in atto nessuna strategia di test, pertanto non si può avere la certezza che l'elevata stabilità delle prestazioni TIC sarebbe effettivamente garantita anche in caso di evento importante. Inoltre, la mancanza di test variati e regolari impedisce di aggiornare l'ITSCM. L'AVI-AIn ha formulato raccomandazioni riguardanti la documentazione insufficiente dell'ITSCM e la mancata organizzazione di test.

24-2 Attività informative svolte attraverso il SPPEs

L'AVI-AIn esamina le interfacce nella collaborazione tra il SIC e l'SPPEs al fine di identificare le attività di intelligence. Su tale base, verificherà la legalità, l'adeguatezza e l'efficacia di questa collaborazione.

Nel 2024 si sono svolte diverse interviste in merito alla competenza dell'AVI-Ain per la vigilanza sull'SPPEs (v. n. 6.4). Questa verifica verrà effettuata nel corso del 2025.

24-3 Organizzazione dei contatti con servizi partner presso il servizio ACE

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
15.05.2024	12.11.2024	27.11.2024	02.12.2024	9

Nessun servizio di intelligence può, da solo, riconoscere tutti i pericoli e garantire la difesa da questi ultimi. Per tale motivo, una collaborazione stretta e basata sulla fiducia con servizi partner è indispensabile. Ciò vale anche per i servizi di intelligence della Svizzera, incluso l'ACE. Nel caso specifico dei settori di compiti in cui opera l'ACE, la situazione è ulteriormente complicata dal fatto che si tratta di un servizio relativamente piccolo, che inoltre non è integrato in organi multilaterali (p. es. [Signals Intelligence] SIGINT Seniors Europe) e che, a causa della posizione geografica della Svizzera, non può accedere a tutti i flussi di segnale alla stregua di altri Paesi. Considerati questi aspetti, i contatti bilaterali a livello operativo con servizi partner selezionati assumono un'importanza ancora maggiore.

Questi contatti sono caratterizzati da un rapporto di dare e avere. L'ACE riceve informazioni, ma deve anche fornire a sua volta informazioni che siano di interesse per il servizio partner.

Questo scambio, pur essendo – come già evidenziato – indispensabile per l'ACE, solleva alcune questioni ed è associato a rischi. In particolare, la natura delle informazioni scambiate potrebbe comportare il rischio di azioni non conformi alla legge da parte del servizio, ma anche il processo e le modalità di gestione dei contatti con i servizi partner presentano rischi in termini di efficacia e adeguatezza.

Per questo motivo, l'AVI-AIn ha deciso, sulla base del piano di controllo 2024, di sottoporre a verifica i contatti dell'ACE con i servizi partner.

Per quanto riguarda le questioni giuridiche, l'AVI-AIn ha potuto constatare che l'ACE si attiene alle disposizioni legali e che intrattiene contatti con i servizi partner nell'ambito dell'intelligence esclusivamente su mandato del SIC. La maggior parte di questi contatti riguarda questioni tecniche. Qualora vengano scambiate anche informazioni più delicate, come i dati, viene preventivamente coinvolto il servizio giuridico del SIC per verificare le basi legali rilevanti per lo scambio dei dati in questione.

Per quanto concerne l'efficacia e l'adeguatezza dei contatti con i servizi partner, l'AVI-AIn è giunta alla conclusione che, **date le circostanze, gli attuali contatti sono organizzati e gestiti in modo efficace. Anche l'approccio adottato per stabilire futuri contatti con i servizi partner nell'ambito delle attività ciber e delle azioni elettromagnetiche sembra essere efficace ed efficiente.** Sebbene, da un punto di vista puramente tecnico, un'integrazione in organi internazionali nel settore SIGINT prometterebbe una maggiore efficacia nell'ambito dei contatti con i servizi partner, tale decisione rappresenta una scelta politica di ampia portata e non può essere presa a livello di ACE o di SIC.

Basandosi sull'impressione generale secondo cui l'ACE si attiene rigorosamente alle basi legali e, data la situazione, trae il massimo dai contatti con i servizi partner, l'AVI-AIn non ha formulato raccomandazioni.

24-11 Aspetti relativi alla sicurezza secondo l'art. 6 cpv. 7 della legge federale del 25 settembre 2015 sulle attività informative (LAIn, RS 121)

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
16.10.2024				2

Il SIC è tenuto a proteggere il suo personale, le sue installazioni, le sue fonti e i dati che tratta. In ambiti selezionati, l'AVI-AIn verifica in che modo il SIC adempie tale obbligo.

Questa verifica non era stata annunciata nel piano di controllo 2024 e sarà completata nel 2025.

5.2.3 Collaborazione

Nell'ambito «Collaborazione» l'AVI-AIn verifica la collaborazione dei servizi con le autorità nazionali e internazionali. L'AVI-AIn verifica ogni anno la collaborazione con alcuni servizi informazioni cantonali (SICant). Con i rapporti di controllo «23-6 SICant Nidvaldo» e «23-7 SICant Obvaldo» nonché con la pubblicazione delle sintesi dei risultati di queste verifiche sul proprio sito web, l'AVI-AIn ha completato la verifica di tutti i Cantoni. Pertanto, può tracciare un bilancio delle verifiche svolte in tutti i 26 Cantoni.

Nel 2024 l'AVI-AIn ha svolto le seguenti verifiche:

23-6 Servizio informazioni cantonale Nidvaldo (SICant NW)

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
16.11.2023	15.02.2024	20.03.2024	10.04.2024	2

L'AVI-AIn ha verificato se la collaborazione tra il SIC e il SICant NW si svolge in modo conforme alla legge, adeguato ed efficace, giungendo alla conclusione che la collaborazione tra i due servizi è buona. Il SICant NW ha di norma eseguito i mandati del SIC in maniera tempestiva e in modo appropriato dal punto di vista del contenuto. Tuttavia, l'AVI-AIn ha avuto l'impressione che il SICant NW non tenga adeguatamente conto della necessaria separazione tra l'infrastruttura della polizia cantonale e quella del SICant, il che comporta il rischio di fughe di informazioni. L'AVI-AIn ha formulato una raccomandazione in merito.

L’AVI-AIn ha inoltre verificato se i dati salvati e i dati personali rispettano le disposizioni legali per quanto riguarda il legame con il compito, il rispetto dei limiti di trattamento nonché la correttezza e la rilevanza delle informazioni. A tale proposito è stato constatato che le questioni irrisolte relative alla gestione dei dati o i problemi tecnici rilevanti per la protezione delle informazioni non vengono affrontati con l’attenzione e la disciplina necessarie, oppure che il legame con il compito non è sempre tracciabile a causa di partenze di personale. Ciò comporta il rischio di un trattamento illecito dei dati e di fughe di informazioni. L’AVI-AIn ha formulato una raccomandazione in merito.

23-7 Servizio informazioni cantonale Obvaldo (SICant OW)

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
16.11.2023	15.02.2024	29.03.2024	16.04.2024	2

L’AVI-AIn ha verificato se la collaborazione tra il SIC e il SICant OW si svolge in modo conforme alla legge, adeguato ed efficace, giungendo alla conclusione che, negli attuali ambiti tematici, la collaborazione tra i due servizi è buona e che la comunicazione funziona anche a bassa soglia. Il SICant OW ha eseguito i mandati del SIC in maniera tempestiva e in modo appropriato dal punto di vista del contenuto e delle risorse. L’AVI-Ain ha avuto l’impressione che il SICant OW disponga di buone conoscenze in materia di intelligence e delle relative qualità e che vi siano i presupposti e la motivazione necessari per l’adempimento dei compiti.

L’AVI-AIn ha inoltre verificato se i dati salvati e i dati personali rispettano le disposizioni legali per quanto riguarda il legame con il compito, il rispetto dei limiti di trattamento nonché la correttezza e la rilevanza delle informazioni. A questo riguardo non sono state constatate anomalie.

Verifiche effettuate presso i SICant negli anni passati

Tra il 2019 e il 2024 l’AVI-AIn ha svolto una verifica presso tutti i SICant. La strategia di verifica è stata la stessa per tutti i SICant, ma per ciascuna verifica sono state aggiunte domande specifiche.

In 11 Cantoni non ci sono state contestazioni. In 15 Cantoni, invece, l’AVI-AIn ha rilevato un potenziale di miglioramento, in particolare per quanto riguarda il trattamento dei dati, l’uso delle risorse e l’impiego degli strumenti tecnici. Ad eccezione di una raccomandazione il cui termine di attuazione non era ancora scaduto, tutte le raccomandazioni formulate nell’ambito dell’ultima verifica sono state attuate. Grazie alle misure adottate dal SIC, alcuni tipi di problematiche che in passato avevano dato adito a contestazioni non sono più state riscontrate nel corso degli anni. Inoltre, talvolta una raccomandazione formulata nei confronti di un Cantone ha avuto effetti anche su altri Cantoni.

Grazie a queste verifiche, l’AVI-AIn dispone di conoscenze approfondite dei SICant, delle loro attività e delle loro peculiarità. Alcune autorità di vigilanza cantonali inviano regolarmente i loro rapporti di vigilanza all’AVI-AIn, integrando così le informazioni a disposizione di quest’ultima.

Per i prossimi anni, l’AVI-AIn ha deciso di svolgere le verifiche presso i SICant non più sulla base di questioni da verificare standardizzate, ma prendendo in considerazione i rischi relativi a temi specifici nei singoli Cantoni (v. anche le visite dell’AVI-AIn presso i Cantoni, n. 7.1).

23-10 Collaborazione del SIC con privati

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
05.09.2023	02.07.2024	15.08.2024	16.12.2024	7

Il SIC collabora con persone private, organizzazioni e imprese. Queste collaborazioni si svolgono nel quadro amministrativo attraverso, ad esempio, relazioni contrattuali ordinarie e sul piano operativo in particolare mediante collaborazioni con persone private, cosiddette «supporter». Queste persone collaborano con il SIC e lo sostengono nello svolgimento dei suoi compiti secondo l’art. 6 LAIn.

In una prima fase, l'AVI-AIn ha analizzato una questione in sospeso in relazione con una verifica del Controllo federale delle finanze (CDF) nell'ambito della collaborazione del SIC con persone private sul piano amministrativo. Pertanto, in occasione di un controllo mediante campionatura, ha analizzato un certo numero di contratti sulle prestazioni conclusi tra il SIC e differenti imprese. È stata verificata anche la contabilità del SIC e sono stati fatti controlli mediante campionatura. Sono stati analizzati anche i pagamenti dissimulati che figuravano nella contabilità del SIC e questo ha permesso, in una seconda fase, di estendere le ricerche dell'AVI-AIn al quadro operativo, focalizzandosi sui supporter del SIC.

L'AVI-AIn ha così analizzato la legalità dei mandati attribuiti ai supporter basandosi sui criteri della LAIn e dell'ordinanza del 16 agosto 2017 sulle attività informative (ordinanza sulle attività informative, OAIn, RS 121.1). Inoltre ha analizzato l'adeguatezza e l'efficacia della collaborazione tra il SIC e i supporter, valutando il management del portafoglio e il management del ciclo di vita dei supporter messi in atto dal SIC.

Infine è stata analizzata la gestione dei rischi e sono state verificate diverse ipotesi. Il raggiramento di misure di acquisizione sottoposte ad autorizzazione in occasione di un mandato affidato a una persona privata, il comportamento illecito di una persona privata, il pagamento a una persona privata senza prestazioni in contropartita o la collaborazione con persone private la cui reputazione potrebbe nuocere al SIC sono altri elementi che sono stati presi in considerazione nel quadro di questa verifica.

Secondo l'AVI-AIn, **la visione d'insieme del SIC sulle persone private con cui collabora e la corrispondente documentazione sono adeguati.** La verifica condotta mostra del resto un miglioramento in questo campo. Tuttavia, secondo le costatazioni dell'AVI-AIn, il trattamento delle lacune in materia di sicurezza nel quadro delle collaborazioni con le persone private deve essere migliorato. Inoltre la prassi nell'ambito operativo per quanto riguarda alcuni compiti attribuiti a persone private può anche essere precisata. Anche se non ha fatto raccomanda-zioni, l'AVI-AIn ha attirato l'attenzione del SIC su questi punti, formulando diversi inviti.

24-4 Collaborazione tra SIC e Segreteria di Stato della migrazione (SEM)

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
17.05.2024	18.12.2024			15

L'AVI-AIn verifica se la collaborazione tra il SIC e la SEM nonché il relativo scambio di dati si svolgono in modo conforme alla legge, efficace e adeguato.

5.2.4 Acquisizione

L'acquisizione di informazioni è un compito fondamentale dei servizi di intelligence, che a tal fine possono utilizzare vari mezzi. I mezzi che incidono in modo più invasivo sui diritti fondamentali – come la sfera privata – delle persone interessate sono oggetto di un'attenzione particolare da parte dell'AVI-AIn. Visti i rischi legati alle attività in questione, le verifiche relative alle operazioni (OP) e alla Human Intelligence (raccolta di informazioni da fonti umane [HUMINT]) si svolgono almeno una volta all'anno. Nel 2024 l'AVI-AIn ha svolto le seguenti verifiche in questo ambito:

23-11 Operazioni, necessità di accertamenti operativi (OPAB) e misure di acquisizione soggette ad autorizzazione (GeBM) del SIC

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
04.05.2023	18.01.2024	13.02.2024	05.03.2024	4

Le operazioni di intelligence (OP) e le OPAB rientrano tra i compiti fondamentali del SIC. Esse sono caratterizzate dal fatto che rispetto alle attività correnti sono più complesse e necessitano di una condotta operativa. Inoltre, nell'ambito delle OP, possono essere richieste anche misure di acquisizione soggette ad autorizzazione (GeBM). La complessità delle OP e delle OPAB comporta

regolarmente dei rischi sul piano dell'efficacia e dell'adeguatezza, e le GeBM, dato che incidono nella sfera privata protetta, implicano sempre un rischio giuridico. Perciò, l'AVI-AIn verifica regolarmente queste attività del SIC.

Per quanto riguarda lo sviluppo del portafoglio delle OP e delle OPAB, rispetto all'anno precedente non ci sono stati cambiamenti significativi. Questo vale sia per i quantitativi sia per i temi trattati. Anche quest'anno il SIC è impegnato nel concludere OP e OPAB in corso già da tempo. Secondo l'AVI-AIn questo modo di procedere corrisponde agli obiettivi e dovrebbe essere mantenuto anche in futuro.

Sono state esaminate cinque OP e undici OPAB per verificare se sono eseguite o sono state eseguite in modo conforme alla legge, adeguato ed efficace. **Sulla base delle attività di verifica svolte, l'AVI-AIn non ha riscontrato alcun indizio che suggerisse che le OP e OPAB esaminate si svolgono o sono state svolte in modo non conforme alla legge, inadeguato o inefficace.**

L'AVI-AIn ha esaminato otto misure autorizzate e approvate, tre urgenti e una rifiutata, per verificare se sono state attuate o meno in conformità alle relative decisioni del Tribunale amministrativo federale (TAF). Sulla base delle attività di verifica svolte, l'AVI-AIn non ha motivo di dubitare che le misure esaminate non siano state attuate nel rispetto delle decisioni prese nel corso dei processi di autorizzazione e approvazione. Non vi sono inoltre indicazioni che il SIC abbia attuato illecitamente singole misure nonostante la decisione negativa.

Sulla base della valutazione complessiva positiva, l'AVI-AIn non ha formulato raccomandazioni.

23-12 Fonti umane (HUMINT) presso il SIC

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
11.08.2023	07.03.2024	01.05.2024	26.06.2024	30

L'ambito HUMINT è uno dei cosiddetti settori «clandestini», ossia quelli in cui la segretezza è un pilastro fondamentale dell'attività. Ciò comporta misure di sicurezza e di protezione particolarmente elevate per quanto concerne il personale (p. es. utilizzo di identità fittizie e/o di coperture per dissimulare l'appartenenza al SIC) e le postazioni di lavoro (dissimulate) nonché i flussi finanziari dissimulati necessari per occultare l'origine delle somme di denaro in questione, gli obblighi di protezione delle fonti e così via. I rischi in questi settori sono molteplici e in continua evoluzione, il che giustifica una verifica annuale da parte dell'AVI-Ain.

In vista della trasformazione e del riorientamento strategico del SIC, l'obiettivo principale dell'AVI-AIn era fare il punto della situazione nel settore HUMINT prima di tale trasformazione. Nell'ambito della verifica 23-12 si è pertanto concentrata in particolare sull'evoluzione del portafoglio di fonti, sia dal punto di vista strategico che in relazione al personale del settore HUMINT, alle capacità di sviluppo e di apprendimento nonché ai progetti in corso. La verifica ha anche offerto l'opportunità di ottenere un'istantanea del funzionamento e delle difficoltà del settore HUMINT prima della trasformazione del SIC. A tal fine, è stato intervistato tutto il personale del settore HUMINT, sia oralmente che per iscritto. Sebbene, nel complesso, il personale sia soddisfatto del proprio lavoro e molto motivato, alcune difficoltà già esistenti e precedentemente constatate dall'AVI-AIn sono destinate ad acuirsi con la trasformazione del SIC.

Lo sviluppo e la digitalizzazione della società in generale sono ulteriori fattori che accrescono la pressione sui settori «clandestini». Alcuni progetti in corso, come una nuova formazione per i gestori delle fonti o un nuovo sistema per la gestione della documentazione, mirano a offrire soluzioni in questo ambito. **In generale, il settore HUMINT ha le capacità, le idee, le risorse e la motivazione necessarie per risolvere i problemi attuali.** L'AVI-AIn ha formulato due raccomandazioni riguardanti la gestione del personale e la valutazione delle informazioni fornite dalle fonti umane.

Infine, dalla verifica è emerso che i dossier selezionati e verificati vengono gestiti in modo conforme alla legge e sono adeguatamente documentati.

23-13 Impiego di agenti virtuali (VirtA) nel SIC

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
14.05.2024	21.11.2024			10

La situazione di minaccia a livello globale è cambiata. Nel settore del terrorismo e dell'estremismo violento, la comunicazione si è spostata da piattaforme pubbliche come Facebook a servizi di comunicazione criptati e gruppi chiusi.

A causa di questo nuovo scenario, diventa per esempio meno efficace il monitoraggio di Internet svolto dal SIC attraverso l'uso di identità virtuali fittizie nel campo del terrorismo e dell'estremismo violento, poiché tale strumento copre principalmente lo spazio pubblico e non consente l'accesso ai servizi di comunicazione e ai gruppi chiusi. Per entrare in tali spazi, l'AVI-AIn ha bisogno di agenti virtuali. Stabilendo contatti con i potenziali obiettivi, questi ultimi riescono infatti a guadagnarsi un livello di fiducia sufficiente per ottenere l'accesso ai forum chiusi.

Per questo motivo, l'AVI-AIn ha verificato se il quadro giuridico per l'impiego degli agenti virtuali fosse chiaramente definito e conosciuto dal personale coinvolto. È stata anche verificata l'adeguatezza dello sviluppo e dell'impiego di agenti virtuali presso il SIC.

Inoltre, l'AVI-AIn ha verificato se il SIC disponesse delle condizioni tecniche e organizzative necessarie per ottenere risultati efficaci nell'ambito dell'intelligence attraverso l'impiego di agenti virtuali, o per valutare correttamente le probabilità di successo sin dall'inizio.

24-5 Operazioni, necessità di accertamenti operativi e misure di acquisizione soggette ad autorizzazione del SIC

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
25.07.2024				10

L'AVI-AIn verifica la garanzia della legalità, dell'adeguatezza e dell'efficacia delle operazioni nella nuova struttura organizzativa. Esamina un numero selezionato di operazioni di intelligence e di necessità di accertamenti operativi per verificarne la legalità, l'adeguatezza e l'efficacia. Inoltre, verifica l'attuazione conforme alle decisioni di un numero selezionato di **misure di acquisizione soggette ad autorizzazione** autorizzate e approvate.

24-6 Fonti umane (HUMINT) presso il SIC

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
29.10.2024				1

L'AVI-AIn esamina due aspetti principali: da un lato, vengono verificati il proseguimento della verifica 23-12 e la questione di come il SIC abbia affrontato e attuato alcuni dei punti critici sollevati dall'AVI-AIn in questo rapporto; dall'altro, si tratta di verificare la legalità della gestione delle fonti (fonti umane e supporter) come pure la legalità e l'adeguatezza della documentazione delle registrazioni relative alla gestione delle fonti.

5.2.5 Risorse

Nell'ambito «Risorse» l'AVI-AIn verifica se vi è un uso adeguato delle risorse da parte dei servizi e se è garantita un'attività informativa efficace. Nel 2024 l'AVI-AIn ha svolto le seguenti verifiche nell'ambito «Risorse»:

24-7 Inventario delle tecnologie dell'informazione e della comunicazione (TIC) presso il SIC

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
22.10.2024				

Nell'ambito delle TIC è importante, per vari motivi, che un'organizzazione disponga di una panoramica dell'hardware utilizzato. Tale panoramica aiuta a gestire i componenti hardware durante il loro intero ciclo di vita e a garantire così un impiego ottimale delle risorse. Inoltre, un inventario sistematico impedisce che, all'interno dell'organizzazione, l'hardware venga acquistato e utilizzato da persone non autorizzate. Proprio quest'ultimo punto comporta per il SIC sia un rischio di reputazione sia il pericolo che i dati vengano trattati illecitamente a causa della mancanza di meccanismi di controllo.

L'AVI-AIn verifica pertanto se il SIC dispone di un inventario del proprio hardware e, in caso affermativo, se viene gestito in modo efficace e adeguato al fine di individuare e prevenire l'acquisizione e l'utilizzo non autorizzati di componenti hardware.

La verifica non riguarda l'intero inventario TIC del SIC, ma si concentra solo sull'hardware IT – collegato al centro di calcolo – che viene utilizzato per la registrazione e il trattamento dei dati nell'ambito dell'intelligence.

24-8 Gestione degli incidenti e dei rischi nel Servizio informazioni militare (SIM)

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
30.01.2024	11.06.2024	10.07.2024	23.07.2024	6

Per via del suo carattere spesso segreto, lo svolgimento di attività informative è legato a rischi specifici. In primo luogo, tali attività possono riguardare l'organizzazione dei lavori, cosa che può trovare espressione per esempio in fughe indesiderate di informazioni e nei corrispondenti rischi di reputazione e per la sicurezza. Però vi sono anche aspetti di carattere giuridico o politico che sono legati a rischi di cui il servizio che svolge le rispettive attività è tenuto a rispondere. In tale contesto la gestione dei rischi riveste un ruolo determinante. Innanzitutto, indica se i rischi legati a un'organizzazione sono stati individuati e se sono state definite misure idonee che, da un lato, portano a una riduzione dei rischi e, dall'altro, aiutano a limitare i danni che si verificherebbero nell'ipotesi in cui un rischio si concretizzasse. In tale contesto è rilevante la questione di sapere in che modo l'organizzazione gestisce incidenti che riguardano i rischi già individuati o la sicurezza generale dell'organizzazione (gestione degli incidenti).

La mancanza o l'incompletezza di un sistema di gestione dei rischi può comportare l'impossibilità per un servizio informazioni di far fronte appieno ai propri compiti per quanto riguarda l'acquisizione di informazioni e ridurre il suo grado di efficacia e di adeguatezza. Nella peggiore delle ipotesi il SIM può ritrovarsi nell'incapacità di fornire le prestazioni a favore dell'Esercito svizzero.

Per questa ragione l'AVI-AIn ha deciso di sottoporre a verifica il sistema di gestione dei rischi e degli incidenti del SIM.

Per quanto riguarda la gestione dei rischi, l'AVI-AIn ha constatato che il SIM dispone di una panoramica completa dei rischi più rilevanti. Un sistema ottimale di gestione dei rischi però presuppone anche che i rischi vengano gestiti attivamente ricorrendo a una procedura strutturata. Vi rientrano tra l'altro l'aggiornamento dei documenti validi nonché lo scambio regolare di informazioni in merito all'evoluzione dei rischi e le discussioni sulle misure da adottare. L'AVI-AIn è dell'avviso che

attualmente queste attività in seno al SIM siano ancora insufficienti, tuttavia per il 2024 è prevista una modifica di queste attività grazie a una nuova concezione dei rischi.

Per quanto concerne la gestione degli incidenti, l'AVI-AIn ritiene che si possa partire dal presupposto che gli incidenti rilevanti sotto il profilo della sicurezza idonei a far aumentare o concretizzare i rischi che derivano dalle attività informative svolte dal SIM vengano rilevati dal SIM in maniera strutturata. Secondo l'AVI-AIn questi incidenti vengono gestiti dal SIM e trovano riflesso nella gestione dei rischi. In effetti, finora il SIM si era trovato a dover gestire un numero relativamente esiguo di incidenti. Tale circostanza aumenta a sua volta il rischio di fare affidamento su un'apparente sensazione di sicurezza. **Per questa ragione l'AVI-AIn è giunta alla conclusione che in fase di revisione della concezione dei rischi occorra inserire anche scenari di esercitazione che comprendano le modalità di gestione di incidenti di sicurezza gravi.**

A causa del grado di maturità del sistema di gestione dei rischi, del numero relativamente esiguo di incidenti rilevanti sotto il profilo della sicurezza e della loro gravità piuttosto bassa, nonché del fatto che i membri del SIM per via della loro esperienza militare presentano un elevato grado di consapevolezza del rischio, l'AVI-AIn ha rinunciato a formulare raccomandazioni.

5.2.6 Trattamento dei dati e archiviazione

Nell'ambito «Trattamento dei dati e archiviazione» l'AVI-AIn verifica in particolare la legalità del trattamento delle informazioni, poiché le informazioni trattate dai servizi sono altamente sensibili e le disposizioni legali sono tanto ampie quanto complesse. Nel 2024 l'AVI-AIn ha svolto le seguenti verifiche nel suddetto ambito:

22-15 Open Source Intelligence (OSINT) presso il SIC

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
29.12.2022	07.12.2023	14.02.2024	08.03.2024	11

L'OSINT è un settore in rapido sviluppo dell'attività di acquisizione di informazioni svolta dai servizi di intelligence. Il collegamento di una quantità inesauribile di dati accessibili pubblicamente (Open Source Information, OSINF) offre ai servizi di intelligence possibilità quasi illimitate di acquisire informazioni. L'analisi delle OSINF, finalizzata a ottenere informazioni utili, è denominata OSINT. L'OSINT è una misura di acquisizione non soggetta ad autorizzazione ai sensi dell'art. 13 LAIn e permette al SIC di cercare informazioni rilevanti per l'intelligence partendo da una grande quantità di dati disponibili.

L'OSINT è in costante sviluppo e solleva questioni di natura giuridica ed etica tra gli addetti ai lavori a livello internazionale, tra cui la delimitazione dell'OSINT rispetto alla ricerca d'informazioni tramite fonti umane (HUMINT), in particolare per quanto concerne l'impiego attivo di identità fittizie per interagire con obiettivi su Internet o per acquisire banche dati offerte illegalmente in rete («leak»). Di conseguenza, l'AVI-AIn ha deciso di esaminare in che modo il SIC affronta i rischi legati all'OSINT.

Secondo l'art. 13 LAIn, sono fonti d'informazione pubbliche soprattutto i media accessibili al pubblico, i registri accessibili alle autorità della Confederazione e dei Cantoni, i dati personali che privati rendono accessibili al pubblico e le dichiarazioni rese in pubblico. Il limite tra OSINT e GeBM non è sempre netto ed è tema di discussione anche presso i servizi partner del SIC e le autorità di vigilanza estere. Senza una concezione comune di questi limiti, si corre il rischio di acquisire dati illecitamente. Dalle interviste realizzate con collaboratori del settore OSINT del SIC è emerso che essi sono consapevoli del fatto che operano in un contesto giuridico complesso. Tuttavia, non esistono criteri o una direttiva strutturata per determinare ciò che è realmente l'OSINT e quali sono i limiti del quadro giuridico di questa attività. Quindi, l'impiego delle varie misure di acquisizione in ambito OSINT non è disciplinato in modo chiaro e uniforme in seno al SIC. L'AVI-AIn ha formulato una raccomandazione con cui chiede di delimitare il quadro giuridico per le attività operative concrete del SIC che si fondano sull'OSINT e di stabilire norme uniformi per l'impiego dell'OSINT.

L’AVI-AIn ha verificato una serie di acquisizioni OSINT selezionate senza trovare elementi che indicassero un’acquisizione illecita di informazioni. Il SIC è tenuto per legge a documentare la sua attività con una gestione degli affari sistematica. Tutti i documenti rilevanti per gli affari devono essere registrati e archiviati nel sistema di gestione elettronica degli affari (GEVER) del SIC. In singoli casi la documentazione degli accertamenti OSINT era lacunosa e non rispettava le vigenti prescrizioni nell’Amministrazione federale, il che ha reso impossibile una valutazione della legalità da parte dell’AVI-AIn. L’AVI-AIn ha formulato una raccomandazione in proposito.

Per poter raccogliere in modo adeguato ed efficace informazioni rilevanti per l’intelligence partendo dall’enorme quantità di dati accessibili pubblicamente su Internet, si utilizzano i cosiddetti «tool OSINT». Il SIC utilizza sia prodotti standard reperibili in commercio sia prodotti sviluppati in proprio.

Con questi tool, e avvalendosi tra l’altro di identità virtuali fittizie (IVF), svolge sia un monitoraggio permanente sia ricerche mirate. Dato che servono per attività di intelligence, le IVF utilizzate presentano anomalie e perciò potrebbero essere considerate come potenziali obiettivi da altri servizi e attirare l’attenzione, per esempio, di servizi partner esteri. Per contrastare questo rischio, l’AVI-AIn ha suggerito al SIC di assicurare almeno con i SICant un’informazione reciproca sulle IVF utilizzate.

Per l’acquisizione di informazioni OSINT anonimizzata, il SIC utilizza un’infrastruttura informatica speciale. Questa infrastruttura presenta lacune di sicurezza e dovrebbe essere sostituita al più presto. L’AVI-AIn ha formulato una raccomandazione in proposito.

La verifica delle informazioni tratte da ricerche OSINT non è sempre cosa semplice, in particolare se le informazioni provengono dal «darknet». Secondo il SIC, le attività di intelligence implicano una sana diffidenza nei confronti delle informazioni acquisite. Se un’informazione non può essere verificata e il grado di veridicità del suo contenuto non può essere quantificato, nei rapporti OSINT questo aspetto viene indicato. Il problema della verifica delle fonti, che assume un ruolo importante per esempio per identificare e svelare le fake news, è noto in particolare nell’impiego di tool OSINT commerciali complessi e se ne discute regolarmente anche all’interno della comunità dei servizi di intelligence.

Oltre al SIC, anche i SICant svolgono accertamenti legati all’OSINT. L’AVI-AIn ha esaminato se esistono ridondanze e inefficienze, giungendo alla conclusione che tutti i servizi sono sensibilizzati in merito ai rischi e ha constatato per esempio che discutono regolarmente la questione dell’OSINT in un contesto creato appositamente.

Il SIC utilizza il sistema d’informazione Portale OSINT per mettere a disposizione al suo interno i dati provenienti da fonti accessibili al pubblico. Le attività di controllo dell’AVI-AIn non hanno fatto emergere indizi di violazione dei principi di adeguatezza o efficacia nella gestione dei dati sul Portale OSINT. Il rischio di prolungamento illecito del termine di conservazione, legato a un’etichettatura sbagliata dei dati come dati OSINT generata da altri sensori, è risultato inesistente, poiché i dati OSINT hanno un termine di conservazione più breve.

22-18 Acquisizione di dati da parte del settore ciber del SIC

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
07.06.2022	18.11.2024			17

Le attività di controllo, particolarmente dispendiose in termini di tempo, sulle questioni ancora irrisolte riguardanti l’acquisizione illecita di informazioni da parte del settore ciber del SIC sono state completate nell’anno in esame. Poiché anche la redazione del rapporto ha richiesto un impegno considerevole, prima della chiusura redazionale del presente rapporto di attività è stato possibile avviare soltanto la relativa procedura di consultazione. Pertanto, in questa sede non è ancora possibile entrare nel merito dei dettagli concreti e dei risultati della verifica. L’AVI-AIn prevede di pubblicare sul proprio sito web la sintesi della verifica nel 2025 e di fornire un resoconto dettagliato nel prossimo rapporto di attività.

23-16 Sistemi d'informazione, sistemi di memorizzazione e memorie di dati non contemplati dall'art. 47 LAIn

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
17.07.2023	18.03.2024	06.05.2024	05.06.2024	7

Fin dalla sua istituzione, l'AVI-AIn controlla a intervalli regolari i sistemi d'informazione del SIC. L'elaborazione dei dati è alla base delle attività del Servizio delle attività informative. Se i dati non vengono elaborati correttamente e se non sono a disposizione del personale per l'analisi e la valutazione della situazione a livello di politica di sicurezza, l'adempimento dei compiti del SIC può essere compromesso. Con la LAIn, per la prima volta i sistemi d'informazione utilizzati dal SIC per lo svolgimento delle proprie attività sono stati regolamentati in un unico punto, ovvero all'art. 47 LAIn.

Nel corso delle proprie attività di controllo, l'AVI-AIn ha riscontrato che vengono utilizzati altri sistemi d'informazione oltre a quelli elencati nell'art. 47 LAIn. L'esaustività dell'elenco di cui all'art. 47 LAIn era già controversa al momento dell'elaborazione della legge. L'AVI-Ain ha voluto chiarire questa questione giuridica ed è giunta alla conclusione che l'elenco è esaustivo in relazione ai dati nei sistemi utilizzati per le attività informative in senso stretto. I dati devono infatti essere salvati in uno dei sistemi d'informazione citati nell'art. 47 LAIn.

L'AVI-AIn ha quindi esaminato quali altri sistemi vengono utilizzati e per quali motivi, cercando di determinare se le basi giuridiche fossero sufficienti. È giunta alla conclusione che le basi giuridiche pertinenti sono sufficienti per il funzionamento di altri sistemi e banche dati.

Dato che il SIC si occupa di così tanti sistemi, è necessario garantire una gestione completa e corretta di ognuno di essi. In particolare, bisogna avere una panoramica completa e aggiornata di tutti i sistemi, al fine di garantire che l'elaborazione dei dati avvenga sempre in modo conforme alla legge. **L'ispezione ha rilevato che la panoramica dei sistemi gestiti che non sono contemplati dall'art. 47 LAIn deve essere adeguatamente aggiornata e mantenuta. Tale panoramica deve essere condivisa tra la direzione, il controllo qualità e i team tecnici per garantire lo svolgimento dei controlli e un'adeguata conservazione dei dati.** In merito a questo tema, l'AVI-Ain ha formulato una raccomandazione.

24-9 Rilevamento a campione IASA-ICC (Integral analysis system control center)

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
09.12.2024				

L'AVI-AIn verifica, sulla base di controlli a campione e interviste, la legalità, l'adeguatezza e l'efficacia dei dati contenuti nel sistema IASA-ICC.

24-10 Ricerche in sistemi d'informazione di terzi da parte del SIC

Mandato	Consultazione	Rapporto definitivo	Lettera di attuazione o conferma di ricezione	Interviste realizzate
10.06.2024				5

L'AVI-AIn verifica se gli accessi a sistemi d'informazione selezionati di terzi e le relative ricerche da parte del SIC vengono effettuati in modo conforme alla legge e adeguato.

5.3 Atteggiamento cooperativo

I responsabili delle verifiche dell'AVI-AIn sono stati ricevuti con atteggiamento costruttivo e professionalità dai servizi sottoposti a vigilanza. Essi hanno potuto accedere senza complicazioni ai documenti e ai sistemi d'informazione necessari per poter adempiere il loro mandato di verifica. Le

persone intervistate erano a loro disposizione. Alle domande complementari è stata data risposta il più rapidamente possibile.

5.4 Controlling delle raccomandazioni

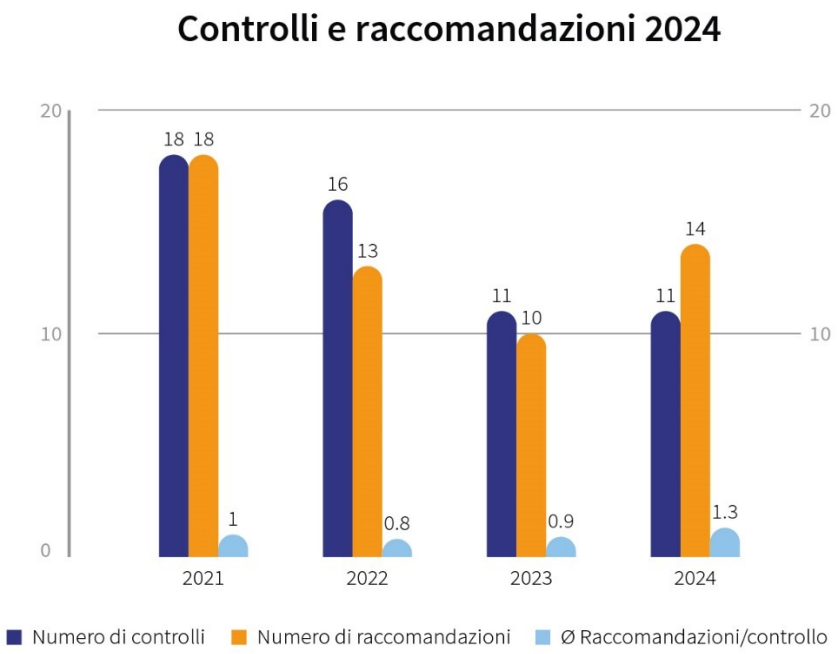
Conformemente alle basi legali, in seguito alle sue attività di controllo l'AVI-AIn può formulare raccomandazioni all'attenzione del capo del DDPS. Successivamente, il DDPS provvede all'attuazione concreta di tali raccomandazioni. Se rifiuta una raccomandazione, il DDPS la sottopone al Consiglio federale per decisione, ma finora ciò non è mai accaduto.

L'AVI-AIn non dispone di prescrizioni legali specifiche per controllare l'attuazione delle raccomandazioni (monitoraggio delle raccomandazioni). Tuttavia, una vigilanza efficace e credibile è garantita solo se, da un lato, le raccomandazioni formulate vengono attuate e, dall'altro, ne viene anche controllata la corretta attuazione. L'AVI-AIn gestisce questa parte della sua attività di vigilanza interagendo con i servizi sottoposti a vigilanza e con il DDPS.

Il grafico qui sotto illustra (per ogni anno in esame) il rapporto tra il numero di verifiche e le conseguenti raccomandazioni negli ultimi quattro anni.

Dopo una fase iniziale di tre anni (2018–2020) con in media due o tre raccomandazioni per verifica, a partire dal 2021 è stata formulata in media una sola raccomandazione per ogni verifica. Questo calo è riconducibile all'attuazione coerente dell'approccio dell'AVI-AIn, che prevede di formulare raccomandazioni meno numerose ma più mirate e orientate ai risultati. Il numero di raccomandazioni non è indice né dei miglioramenti ottenuti né di un peggioramento della situazione.

	2018-2020	2021	2022	2023	2024
Numero di controlli	49	18	16	11	11
Numero di raccomandazioni	150	18	13	10	14
Ø Raccomandazione/controllo	3,1	1,0	0,8	0,9	1,3



6 Sguardo all’interno dell’AVI-AIn

Nel presente capitolo l’AVI-AIn riferisce in merito ad affari interni.

6.1 Personale

Nel 2024 l’AVI-AIn disponeva di un effettivo di nove collaboratori. Nel corso dell’anno una persona ha lasciato l’AVI-AIn ed è stata sostituita da una nuova persona.

6.2 Formazioni e formazioni continue

Nel corso del 2024 il personale dell’AVI-AIn ha seguito numerose formazioni e formazioni continue organizzate dalla Confederazione o da istituzioni private, in particolare negli ambiti della gestione dei rischi, degli audit, della cibersicurezza e dello sviluppo personale. Inoltre, sono stati completati con successo due formazioni continue sotto forma di CAS (Certificate of Advanced Studies): un CAS in comunicazione e uno in gestione dell’intelligenza artificiale.

6.3 Accesso a documenti e informazioni ufficiali

L’AVI-AIn, in quanto parte dell’Amministrazione federale decentralizzata, opera su mandato della cittadinanza, che ha il diritto di sapere cosa fanno le autorità e in che modo adempiono il loro mandato. Da questo principio derivano, da un lato, il diritto della cittadinanza di accedere alle informazioni, e dall’altro il dovere, da parte delle autorità, di fornire tali informazioni.

Nell'anno di riferimento, l’AVI-AIn ha ricevuto undici richieste di accesso rivolte all'autorità stessa. L'accesso è stato negato in sei casi, parzialmente concesso in due casi e pienamente concesso in due casi. Inoltre, in un caso è stata richiesta l'assistenza dell'AVI-Ain per l'elaborazione di una domanda ai sensi della legge federale del 17 dicembre 2004 sul principio di trasparenza dell’amministrazione (Legge sulla trasparenza, LTras, RS 152.3), indirizzata a un altro ufficio dell'Amministrazione federale.

6.4 Competenza dell’AVI-AIn per la vigilanza sull’SPPEs

Durante la consultazione sul piano di controllo 2024 è stata sollevata la questione se l’AVI-AIn fosse competente per la verifica «24-2 Attività informative svolte attraverso il Servizio per la protezione preventiva dell’esercito (SPPEs)».

Nel corso del 2024, il capo del DDPS ha informato l’AVI-AIn di aver presentato tale questione all’Ufficio federale di giustizia (UFG), il quale ha riconosciuto nel suo parere la competenza dell’AVI-AIn per la vigilanza sull’SPPEs in tre situazioni:

- quando l’SPPEs adempie un mandato del SIM;
- quando l’SPPEs adempie un mandato del SIC; e
- quando l’SPPEs svolge attività che servono contemporaneamente all’adempimento di compiti secondo gli art. 99 e 100 della legge federale del 3 febbraio 1995 sull’esercito e sull’amministrazione militare (Legge militare, LM; RS *510.10*) o quando nella pratica non è possibile stabilire se un’attività serva ad adempiere un compito secondo gli art. 99 e 100 LM.

Il capo del DDPS ha comunicato all’AVI-AIn che la questione della competenza potrebbe essere trattata nell’ambito della revisione della LM nel 2029.

L’AVI-AIn ha preso atto del parere dell’UFG, che nel complesso coincideva con la propria valutazione giuridica, ed è giunta alla conclusione che la verifica 24-2, il cui obiettivo principale era esaminare la collaborazione tra il SIC e l’SPPEs, non è stata messa in discussione. L’AVI-AIn ha inoltre dichiarato che, nella pianificazione delle sue future verifiche, terrà conto anche dell’interpretazione giuridica dell’UFG.

6.5 Revisione della LAIn

La revisione della LAIn, iniziata nel 2020, procede secondo i piani. È stata suddivisa in due pacchetti. La prima parte («pacchetto di base») riguarda in particolare il trattamento dei dati da parte del SIC e l'attività di vigilanza. La procedura di consultazione si è svolta nell'estate del 2022 e il Consiglio federale adotterà all'attenzione del Parlamento il messaggio relativo al pacchetto di base entro la fine del 2025. Questa parte del progetto di revisione interessa in modo particolare l'AVI-AIn poiché prevede il trasferimento a quest'ultima dei compiti dell'Autorità di controllo indipendente per l'esplorazione radio e l'esplorazione dei segnali via cavo (ACI). Nell'autunno del 2024, nell'ambito della consultazione interna al DDPS, l'AVI-AIn ha richiesto alcune modifiche alle norme riguardanti tale aspetto. Le modifiche in questione mirano a migliorare la leggibilità della legge, a definire in modo coerente l'attività di vigilanza e a includere i nuovi requisiti in materia di protezione dei dati.

Il secondo pacchetto («revisione ciber») serve ad adeguare le disposizioni concernenti il trattamento dei dati in ambito ciber. Entro luglio 2025 è prevista una procedura di consultazione supplementare.

7 Coordinamento

Conformemente all'art. 78 cpv. 2 LAIn, l'AVI-AIn deve coordinare la sua attività con le attività di vigilanza parlamentare e con altri servizi di vigilanza della Confederazione e dei Cantoni.

7.1 Contatti nazionali

Delegazione delle Commissioni della gestione (DelCdG)

La DelCdG ha invitato l'AVI-AIn a una consultazione, in occasione della quale si è discusso in particolare della prassi dell'AVI-AIn in materia di raccomandazioni e relativo monitoraggio, della revisione della LAIn e del piano di controllo 2025.

Tribunale amministrativo federale (TAF)

Nell'anno in esame, le rappresentanti e i rappresentanti del TAF e dell'AVI-AIn si sono incontrati per due riunioni. Durante questi incontri è stata discussa la prassi del tribunale riguardo alle misure GeBM e alle richieste di esplorazione dei segnali via cavo e sono stati inoltre presentati il piano di controllo 2024 dell'AVI-AIn e le verifiche in corso. Inoltre, è stato chiarito il coinvolgimento dell'AVI-AIn nella procedura di autorizzazione e sono stati discussi alcuni punti della revisione della LAIn. È emerso che la prassi del TAF si è dimostrata efficace per quanto concerne le problematiche tecniche, tanto che ormai non si verificano quasi più problemi. In relazione alla revisione della LAIn, il capo dell'AVI-AIn ha presentato la sua recente proposta di trasmettere il rapporto annuale del TAF all'AVI-AIn per un controllo incrociato. Il TAF ha ritenuto ragionevole tale proposta.

Controllo federale delle finanze (CDF)

L'AVI-AIn coordina la sua attività di vigilanza con altre autorità di controllo, in particolare con il CDF.

In questo contesto e a seguito della valutazione dei contratti di prestazioni tra il SIC e i fornitori privati da parte del CDF, è stato allestito un coordinamento mirato. L'AVI-AIn ha svolto una verifica della collaborazione del SIC con privati (23-10) concentrandosi principalmente sui settori «clandestini», che non sono regolati dai consueti contratti di prestazioni. La verifica 23-10 ha peraltro permesso di verificare i contratti non dissimulati e l'attuazione della raccomandazione del CDF. Non sono stati riscontrati problemi significativi nella gestione dei contratti di prestazioni. L'AVI-AIn ha comunicato al CDF i punti rilevanti del suo rapporto affinché ne prendesse atto e vi desse seguito.

In considerazione dell'ampio processo di trasformazione che il SIC sta attualmente attraversando, l'AVI-AIn ha rafforzato i propri scambi con il CDF, come dimostrato dalla condivisione dei risultati delle verifiche e dall'ottimizzazione delle risorse evitando verifiche doppie.

Questa intensificazione del coordinamento testimonia la volontà di entrambe le autorità di vigilanza di garantire una vigilanza completa ed efficace sul SIC e contribuisce a verificare l'attuazione delle raccomandazioni nonché a seguire da vicino la trasformazione del SIC.

Autorità di controllo indipendente per l'esplorazione radio e l'esplorazione dei segnali via cavo (ACI)

Nell'anno in esame si è tenuto un incontro tra il presidente dell'ACI e il capo dell'AVI-AIn, che hanno discusso degli scambi con il TAF e di un possibile incontro tra l'ACI e un'autorità di vigilanza estera in merito all'esplorazione dei segnali via cavo.

In seguito al trasferimento dei compiti dell'ACI all'AVI-AIn previsto nel progetto di revisione della LAIn, anche nel 2024 un rappresentante dell'AVI-AIn ha partecipato a tutte e cinque le sedute dell'ACI. Lo scopo della partecipazione era raccogliere informazioni sui metodi di verifica dell'ACI e garantire il trasferimento di know-how.

Incaricato federale della protezione dei dati e della trasparenza (IFPDT)

Nel 2024 si è tenuta una riunione di coordinamento tra l'AVI-AIn e l'IFPDT. L'AVI-AIn ha informato l'IFPDT sui principali risultati delle sue verifiche concluse e lo ha aggiornato anche su quelle in corso e pianificate che riguardano il trattamento di dati. Si è inoltre discusso dell'attuazione del diritto d'accesso secondo la LAIn.

Visite dell'AVI-AIn presso i Cantoni

Dopo l'entrata in vigore della LAIn, l'AVI-AIn ha svolto un sondaggio presso gli organi di vigilanza cantonali in merito ai SICant e è stata organizzata una prima conferenza con tali organi per discutere dei relativi risultati. I Cantoni hanno partecipato numerosi (cfr. il Rapporto di attività 2018 dell'AVI-AIn). Nell'agosto del 2021 l'AVI-AIn ha organizzato una seconda conferenza per promuovere la formazione continua, il networking e lo scambio di esperienze. Il numero di partecipanti è stato inferiore, ma in compenso sono stati discussi in modo approfondito temi specifici (cfr. Rapporto di attività 2021 dell'AVI-AIn).

Nell'estate del 2024 ha preso il via il ciclo di visite dell'AVI-AIn presso i Cantoni, che durerà fino all'inizio dell'estate del 2025. Gli interlocutori sono i responsabili – ed eventualmente anche il personale specializzato – dei SICant nonché i relativi organi di vigilanza cantonali. Questi ultimi presentano ancora una significativa varietà di forme a livello federale.

Sono previsti i seguenti temi di discussione:

- feedback sulla prima tornata di verifiche presso i SICant da parte dell'AVI-AIn;
- temi attuali di interesse per i SICant e gli organi di vigilanza cantonali in materia di intelligence;
- coordinamento: eventuali ridondanze tra i diversi organi di vigilanza (SIC, AVI-AIn, organi di vigilanza cantonali ecc.), eventuale necessità di vigilanza ed eventuali questioni irrisolte sollevate dagli organi di vigilanza cantonali;
- collaborazione tra SICant e organi di vigilanza cantonali.

Finora i Cantoni hanno accolto favorevolmente le visite e i colloqui si sono rivelati utili e preziosi. Al termine delle visite l'AVI-AIn redigerà un rapporto e approfondirà i punti salienti con il SIC.

Ulteriori incontri

- Capo dell'esercito
- segretario generale del DDPS
- sost. segretario generale del DDPS
- direttore del SIC
- capo del Comando Operazioni
- capo del SIM
- capo dell'ACE
- capo della Revisione interna DDPS
- procuratore generale della Confederazione
- presidentessa dell'Autorità di vigilanza sul Ministero pubblico della Confederazione (AV-MPC)

- direttore CDF
- Responsabile CDF per il settore DDPS
- consulente del DDPS in materia di intelligence;
- i membri dell'ACI

Richieste della cittadinanza

Nel 2024 l'AVI-AIn ha ricevuto 16 richieste da parte della cittadinanza.

7.2 Contatti internazionali

Riguardo a metodi, processi ed esperienze di vigilanza, l'AVI-AIn ha modo di confrontarsi con autorità di vigilanza di altri Paesi che operano nello stesso campo di attività. Ciò si rivela essere un valore aggiunto costante per le attività di verifica. Nel 2024 si sono tenuti i seguenti incontri internazionali:

Intelligence Oversight Working Group (IOWG), incontro tecnico e tra collaboratrici e collaboratori delle autorità, 10–12 aprile 2024, Bruxelles

In preparazione all'incontro periodico tra collaboratrici e collaboratori delle autorità, gli organizzatori belgi hanno svolto per la prima volta un incontro tecnico («technical meeting»). A questa nuova piattaforma di scambio hanno partecipato principalmente specialiste e specialisti delle autorità di vigilanza con solide conoscenze tecniche. L'attenzione si è concentrata su questioni relative all'IA:

- che cosa intendono le autorità di vigilanza per IA?
- L'uso dell'IA o dell'apprendimento automatico è già considerato nelle leggi vigenti?
- Questa tecnologia è già in uso nei servizi sottoposti a vigilanza?
- L'uso di questa tecnologia rientra nell'obbligo di vigilanza delle autorità di vigilanza?
- Le stesse autorità di vigilanza utilizzano attivamente questa tecnologia?
- In che modo le autorità di vigilanza garantiscono il mantenimento e lo sviluppo delle conoscenze sulle nuove tecnologie?

Lo scambio tra le specialiste e gli specialisti si è rivelato molto arricchente, motivo per cui in futuro si prevede di organizzare periodicamente anche gli incontri tecnici.

Dopo l'incontro tecnico si è tenuto l'incontro tra collaboratrici e collaboratori delle autorità, con rappresentanti delle autorità di vigilanza di Belgio, Danimarca, Paesi Bassi, Norvegia, Inghilterra, Svezia e Svizzera. Era presente anche l'autorità canadese NSIRA (National Security and Intelligence Review Agency), con lo statuto di osservatore.

All'inizio dell'evento, le partecipanti e i partecipanti hanno presentato vari sviluppi in materia di intelligence registrati nei rispettivi Paesi dall'ultimo incontro tenutosi nel 2023. Si sono svolte vivaci discussioni sui seguenti temi:

- vigilanza sulle indagini dei servizi di intelligence contro politici e funzionari eletti, prendendo come esempio un caso attuale di pubblico dominio Belgio;
- Convenzione 108+ del Consiglio d'Europa, che disciplina la protezione e lo scambio transfrontaliero di dati personali: ogni Paese partecipante ha riferito in merito al proprio stato di ratifica. Inoltre, si è discusso degli effetti che la Convenzione 108+ avrà su una possibile collaborazione transfrontaliera in materia di intelligence (sia per i servizi che per le autorità di vigilanza);
- matrice di controllo dei rischi presentata dall'autorità canadese NSIRA e finalizzata a stabilire le priorità tra i compiti di verifica.

IOWG: incontro tecnico e tra collaboratrici e collaboratori delle autorità, 23–25 ottobre 2024, Stoccolma

Durante l'incontro tecnico, tutte le autorità di vigilanza partecipanti hanno presentato per la prima volta esempi concreti tratti dalla loro esperienza pratica nei rispettivi Paesi e riguardanti la gestione di grandi volumi di dati. Le partecipanti e i partecipanti hanno così potuto beneficiare delle esperienze e delle competenze specialistiche di altri Paesi, dando vita a vivaci discussioni.

Anche l’incontro tra collaboratrici e collaboratori delle autorità, dopo le relazioni sugli sviluppi nei Paesi partecipanti, è stato incentrato sulla gestione di grandi volumi di dati, ma – rispetto all’incontro tecnico – l’attenzione si è focalizzata su una prospettiva non tecnica. Ogni Paese partecipante ha per esempio illustrato la propria situazione giuridica attuale per quanto concerne la vigilanza sul trattamento di grandi volumi di dati da parte dei servizi di intelligence.

Questo incontro internazionale a Stoccolma ha chiaramente evidenziato come tutti i Paesi siano impegnati su temi simili, tra cui l’aumento del personale nei servizi di intelligence, una maggiore trasparenza mediatica dei servizi e la revisione delle basi giuridiche.

8 Allegato

8.1 Piano di controllo 2024

N.	Titolo	Organo verificato
Strategia e pianificazione		
24-1	Intelligenza artificiale	SIC
Organizzazione e attribuzione di mandati		
24-2	Attività informative svolte attraverso il Servizio per la protezione preventiva dell'esercito (SPPEs)	SIC / SIM & SPPEs
24-3	Organizzazione dei contatti con servizi partner presso il servizio ACE	SIC / ACE
Collaborazione		
24-4	Collaborazione tra SIC e Segreteria di Stato della migrazione	SIC
Acquisizione		
24-5	Operazioni / accertamenti operativi / Misure di acquisizione soggette ad autorizzazione	SIC
24-6	Fonti umane (HUMINT)	SIC
Risorse		
24-7	Inventario TIC	SIC
24-8	Gestione degli incidenti e dei rischi nel SIM	SIM
Trattamento dei dati / archiviazione		
24-9	Rilevamento a campione IASA ICC	SIC
24-10	Consultazione dei sistemi di informazione di terzi	SIC

8.2 Elenco delle abbreviazioni

ACE	Servizio delle attività ciber ed elettromagnetiche
ACI	Autorità di controllo indipendente per l'esplorazione radio e l'esplorazione dei segnali via cavo
Art.	Articolo
AV-MPC	Autorità di vigilanza sul Ministero pubblico della Confederazione
AVI-AIn	Autorità di vigilanza indipendente sulle attività informative
BCM	Business Continuity Management
CAS	Certificate of Advanced Studies
CDF	Controllo federale delle finanze
Cfr.	Confronta
Cpv.	Capoverso
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DelCdG	Delegazione delle Commissioni della gestione
GeBM	Misure di acquisizione soggette ad autorizzazione
GEVER	Geschäftsverwaltungssystem, sistemi di gestione degli affari
HUMINT	Human Intelligence, acquisizione di informazioni per mezzo di fonti umane
IASA ICC	Integral analysis system control center
IFPDT	Incaricato federale della protezione dei dati e della trasparenza
IOWG	Intelligence Oversight Working Group
IT	Information Technology, tecnologia dell'informazione
ITSCM	IT Service Continuity Management
IVF	Identità virtuali fittizie
LAin	Legge federale del 25 settembre 2015 sulle attività informative (RS 121)
LM	Legge federale del 3 febbraio 1995 sull'esercito e sull'amministrazione militare (Legge militare, RS 510.10)
LTras	Legge federale del 17 dicembre 2004 sul principio di trasparenza dell'amministrazione (Legge sulla trasparenza, RS 152.3)
NW	Nidvaldo
n.	Numero
OAIn	Ordinanza del 16 agosto 2017 sulle attività informative (RS 121.1)
OP	Operazioni di intelligence
OPAB	Necessità di accertamenti operativi
OSINF	Open Source Information
OSINT	«Open Source Intelligence», messa a disposizione di dati provenienti da fonti accessibili al pubblico
OW	Obvaldo
p. es.	Per esempio
RS	Raccolta sistematica delle leggi federali
SEM	Segreteria di Stato della migrazione
SIC	Servizio delle attività informative della Confederazione
SICant	Servizi informazioni cantonali
SIGINT	Signal Intelligence
SIM	Servizio informazioni militare della Confederazione
Sost.	Sostituto
SPPEs	Servizio di protezione preventiva dell'esercito
TAF	Tribunale amministrativo federale
TIC	Tecnologie dell'informazione e della comunicazione
UFG	Ufficio federale di giustizia
VirtA	Agente virtuale