



PRESIDENZA DEL CONSIGLIO DEI MINISTRI
Sistema di informazione per la sicurezza della Repubblica

IL LINGUAGGIO
DEGLI
ORGANISMI INFORMATIVI

Intelligence

Glossario



PRESIDENZA DEL CONSIGLIO DEI MINISTRI
Dipartimento delle Informazioni per la Sicurezza

Gnosis

RIVISTA ITALIANA DI INTELLIGENCE



IL LINGUAGGIO
DEGLI
ORGANISMI INFORMATIVI

Glossario intelligence

PREMESSA

Linguaggio ed intelligence hanno entrambi a che fare con le informazioni: l'uno è lo strumento attraverso cui si comunicano informazioni, l'altra è l'attività che per definizione si sostanzia nella ricerca ed elaborazione di informazioni.

Tale riflessione basterebbe di per sé a spiegare il senso di questo primo tentativo di mettere a punto un glossario del Sistema di informazione per la sicurezza della Repubblica, vale a dire del complesso di organi ed uffici cui è affidato, in Italia, l'insieme di attività che vengono oggi usualmente indicate con il termine intelligence.

Un vocabolo che rappresenta ciò che viene definito "prestito linguistico", ed anzi un insolito prestito "bidirezionale": di conio anglosassone, il termine vanta infatti un'evidente etimologia latina (in quanto derivante dall'intelligere della lingua dei Cesari) e torna poi ad essere impiegato anche presso di noi nella duplice accezione che gli è propria: l'una, soggettiva, che rimanda al complesso delle strutture e delle attività volte a raccogliere notizie utili ai fini della tutela della sicurezza nazionale; l'altra, oggettiva, che si riferisce al prodotto di tale attività, funzionale a sostenere le decisioni in materia di protezione degli interessi del Paese. Sono queste le informazioni di cui parla il Legislatore nella legge istitutiva del Sistema di informazione per la sicurezza della Repubblica e che compaiono frequenti nel Glossario proprio per rispettare tale scelta lessicale.

Ciò non toglie che, grazie alla natura veicolare dell'idioma di origine, intelligence si sia di fatto affermato come il lemma a

valenza generale usato oggi per definire un'attività che è in realtà antichissima. Oltre all'esempio, assai noto, degli scritti dello stratega cinese Sun Tzu – che già nel VI secolo a.C. teorizzava l'impiego di "spie" – vale la pena ricordare che era sicuramente informativa la missione che, secondo la Bibbia, Mosè affidò a dodici "agenti" ante litteram, incaricandoli di esplorare la terra di Canaan.

Se dunque estremamente risalente è la necessità dei decisori politici di disporre di elementi di conoscenza dettagliati su minacce, pericoli ed opportunità, altrettanto lunga è la storia dell'attività volta a procacciare tali elementi. Come avviene per ogni arte e mestiere, l'intelligence ha nel tempo sviluppato un proprio linguaggio ed un proprio gergo, frutto di una costante evoluzione sulla quale influisce una pluralità di fattori, primi fra tutti il mutare delle condizioni operative e gli interventi legislativi che dell'attività di informazione per la sicurezza dettano disciplina ed organizzazione.

Non è un caso che la presente pubblicazione veda la luce dopo una legge di riforma che ha introdotto, tra i compiti del Dipartimento delle Informazioni per la Sicurezza, la promozione e diffusione della cultura della sicurezza, al fine di propiziare, con il superamento dei luoghi comuni che troppo spesso segnano il discorso pubblico sull'intelligence, anche una nuova, costruttiva dimensione del rapporto tra comparto informativo e società. Una nuova dimensione che passa necessariamente per una demistificazione dell'intelligence e per una corretta definizione di ciò che essa è – un microcosmo di uomini e donne che, all'interno di un quadro disciplinato dalla legge, lavorano per garantire la sicurezza della collettività nazionale – e, forse soprattutto, di ciò che essa non è, con buona pace delle finzioni e delle iperboli letterarie e cinematografiche.

In una fase in cui è fortemente avvertita l'esigenza di "saper dare un nome" alle cose, quelle che seguono vanno lette come pagine contenenti i vocaboli principali utilizzati dalla comunità intelligence italiana, in un'elencazione, certamente non esaustiva, intesa a fornire un contributo ad un più corretto inquadramento del quotidiano operare delle strutture chiamate a garantire la sicurezza nazionale. Un contributo volto, in definitiva, a chiarire che gli organismi informativi possono riconoscersi nell'espressione "servizi segreti", con cui sono spesso definiti, solo in quanto di essa si colga e venga valorizzata la funzione di "servizio" a favore del Paese.

In quest'ottica "Il linguaggio degli organismi informativi - Glossario intelligence" si prefigge di "accendere una luce", vivida e chiara, su ambienti che nulla hanno in realtà di misterioso, ma per i quali il "segreto" ha l'unica valenza di strumento a tutela di una funzione vitale dello Stato democratico.

NOTA METODOLOGICA

“Il linguaggio degli organismi informativi - Glossario intelligence” consiste di n. 259 lemmi definiti sulla base di principi metodologici ispirati dalla finalità divulgativa della pubblicazione e relativi a:

- ostensibilità. Nella definizione dei termini che tratteggiano l'attività di informazione per la sicurezza ci si è attenuti a definizioni e dottrina prevalente, evitando dettagli e peculiarità operative dei singoli organismi o del Sistema di informazione nel suo complesso;
- fruibilità. In quest'ottica è stato privilegiato un registro linguistico improntato a semplicità, rifuggendo da eccessivi tecnicismi. Analogamente si è proceduto nell'interpolare i testi normativi di riferimento – di cui si è peraltro tenuto costantemente conto, adottando un'impostazione coerente con le scelte lessicali della legge 124/2007 – specie quando si è ritenuto potesse essere fonte di ambiguità.

Sulla base dei citati principi, inoltre, la pubblicazione è stata circoscritta ai lemmi caratteristici del comparto (evitando ad esempio vocaboli suggestivi, ma “romanzeschi”) o che in quel contesto assumono peculiari accezioni, tenendo costantemente presente la necessità di consentire al lettore “profano” di cogliere le tipicità dell'attività svolta dal Sistema (talora, come nel caso delle discipline che rimandano al settore economico-finanziario, si è operato “per sottrazione”, definendo cioè l'intelligence economico-finanziaria ma non la *business intelligence* né la *competitive intelligence*, entrambe dominio del settore privato).

Esigenze di sintesi, inoltre, hanno indotto a limitare taluni ambiti – come quelli relativi alle minacce alla sicurezza nazionale – alle sole macrocategorie di riferimento.

In **arancio** i lemmi cui si fa rimando.

A

ABILITAZIONE DI SICUREZZA

Atto rilasciato in favore di una persona, fisica o giuridica, previo accertamento della sua **affidabilità**, che la abilita all'**accesso** alle informazioni con classifica superiore a RISERVATO. Assume denominazioni diverse – **Abilitazione Preventiva, Nulla Osta di Sicurezza, Nulla Osta di Sicurezza Industriale** – a seconda del soggetto a favore del quale è rilasciata e del tipo di attività autorizzata.

ABILITAZIONE PREVENTIVA

Abilitazione di sicurezza di cui devono essere dotati gli operatori economici per partecipare a gare d'appalto o a procedure per l'affidamento di contratti classificati RISERVATISSIMO. È rilasciata dall'**Ufficio Centrale per la Segretezza** ed ha validità semestrale.

Vedi anche **NULLA OSTA DI SICUREZZA INDUSTRIALE**

ACCESSO

- a) In tema di tutela della sicurezza delle informazioni, indica la possibilità di prendere conoscenza di informazioni classificate. Tale possibilità è subordinata, oltre che al possesso del Nulla Osta di Sicurezza quando richiesto, al principio della **necessità di conoscere** ed alla cognizione delle misure poste a protezione delle informazioni classificate e delle connesse responsabilità.
- b) La prossimità di una **fonte confidenziale** alla notizia e quindi la sua concreta possibilità di apprenderla e riferirla in modo attendibile: si parla in gergo di fonte

con “accesso diretto” ovvero con “accesso indiretto”, quando la fonte riferisce notizie apprese da terzi.

ACCORDO DI COOPERAZIONE/COLLABORAZIONE

Insieme di previsioni pattizie che definiscono gli ambiti della **collaborazione internazionale intelligence** tanto a livello bilaterale che multilaterale. Avendo frequentemente carattere informale, assume spesso la veste di *Gentlemen's agreement*, *Memorandum of Understanding* (MoU), etc.

ACCORDO DI SICUREZZA

Atto internazionale bilaterale o multilaterale, concluso con Paesi esteri e/o con Organizzazioni internazionali o comunitarie, diretto a stabilire regole e procedure comuni per la reciproca protezione e per lo scambio di informazioni classificate.

ACINT (ACOUSTICAL INTELLIGENCE)

Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale provenienti da segnali emessi da ogni tipo di fonte acustica.

ACQUISIZIONE INFORMATIVA

- a) Termine impiegato come sinonimo di **ricerca informativa**.
- b) Il risultato della ricerca informativa.

AFFIDABILITÀ

Grado di fiducia che, in base all'esito delle verifiche effettuate ai fini della concessione, del mantenimento e del rin-

novo di un'abilitazione di sicurezza, si può riporre in una persona fisica o giuridica per quanto riguarda la scrupolosa fedeltà alle istituzioni della Repubblica, alla Costituzione ed ai suoi valori nonché il rigoroso rispetto del segreto.

AGENTE

Termine che indica tanto un appartenente ad un servizio di informazione quanto un soggetto esterno da questo reclutato, addestrato ed impiegato per operare a suo favore.

AGENTE DOPPIO

Agente che, fingendo di operare per conto di un'agenzia intelligence, agisce in realtà a favore di un altro servizio di informazione o di un'entità ostile.

AGENTE DI INFLUENZA

Soggetto che opera sulla base delle direttive di un servizio di informazione e, sfruttando la propria posizione, cerca di influenzare un individuo o un gruppo in senso favorevole all'organizzazione sponsor.

Vedi anche **INFLUENZA**

AGENZIA INFORMAZIONI E SICUREZZA ESTERNA (AISE)

Organismo del Sistema di informazione per la sicurezza della Repubblica cui è affidato il compito di tutelare la sicurezza nazionale svolgendo attività di informazione per la sicurezza nei confronti delle minacce provenienti dall'estero e al di fuori del territorio italiano. Ha competenza esclusiva in materia di controproliferazione. Dipende dal Presidente del Consiglio dei ministri che ne nomina

il Direttore, sentito il Comitato interministeriale per la sicurezza della Repubblica.

AGENZIA INFORMAZIONI E SICUREZZA INTERNA (AISI)

Organismo del Sistema di informazione per la sicurezza della Repubblica cui è affidato il compito di tutelare la **sicurezza nazionale** svolgendo **attività di informazione per la sicurezza** nei confronti delle minacce che su di essa gravano all'interno del territorio italiano. Dipende dal Presidente del Consiglio dei ministri che ne nomina il Direttore, sentito il Comitato interministeriale per la sicurezza della Repubblica.

AGENZIA INTELLIGENCE

Vedi **SERVIZIO DI INFORMAZIONE**

AGENZIA NAZIONALE DI DISTRIBUZIONE

Agenzia preposta alla gestione del materiale crittografico. In ambito nazionale è istituita presso l'**Ufficio Centrale per la Segretezza**.

AGENZIE

Termine colloquiale impiegato per indicare l'**Agenzia informazioni e sicurezza esterna** e l'**Agenzia informazioni e sicurezza interna**.

AISE

Vedi **AGENZIA INFORMAZIONI E SICUREZZA ESTERNA**

AISI

Vedi AGENZIA INFORMAZIONI E SICUREZZA INTERNA

ALL-SOURCE INTELLIGENCE

Informazioni derivanti dall'impiego di tutte le fonti disponibili, per esempio attraverso l'integrazione delle notizie fornite da fonti confidenziali con quelle tratte da fonti aperte.

ANALISI

a) Complesso delle attività logico-concettuali grazie alle quali una o più informazioni acquisiscono rafforzata valenza conoscitiva. Ciò in esito ad una serie di passaggi – integrazione, interpretazione e valutazione – in cui si procede a confrontare l'informazione con il patrimonio informativo, integrarla di dati già validati eventualmente tratti da altre fonti, determinarne la pregnanza, valutare il significato che essa assume nel tratteggiare possibili linee di sviluppo e sistematizzarla all'interno di elaborati di taglio situazionale o previsionale.

La dottrina distingue l'analisi, a seconda delle finalità, in tattica, operativa e strategica. Quest'ultima, volta a sostenere l'adozione di politiche nazionali su questioni di rilevanza strategica, si caratterizza in genere per un marcato carattere previsionale. Analoga, accentuata dimensione previsionale ha la cd. "analisi di scenario", che descrive, attraverso l'uso di tecniche di simulazione, l'evoluzione di fenomeni e minacce o le potenziali linee d'azione di attori di interesse, ipotizzando opzioni alternative (scenari) e valutandone il relativo grado di probabilità. L'esigenza di disporre di quadri di analisi

ad ampio spettro sul panorama complessivo delle minacce alla sicurezza nazionale ha indotto il Legislatore italiano ad introdurre la categoria delle “analisi globali” affidate al Dipartimento delle informazioni per la sicurezza. Si tratta di elaborati analitici che considerano fenomeni, processi e situazioni nel loro insieme, secondo un approccio multidisciplinare. Ulteriore distinzione si basa sulla “finestra temporale” presa in esame dall’attività di analisi: in questo contesto all’analisi strategica vengono frequentemente giustapposte l’analisi cd. “di breve periodo” e quella cd. “di primo impatto”.

b) In un’accezione ristretta indica il **prodotto intelligence** risultante dal processo di analisi.

Vedi anche **ANALISTA**, **CICLO INTELLIGENCE** ed **ELABORAZIONE**

ANALISI DELLE IPOTESI CONFLIGGENTI

Metodo di analisi consistente nell’identificazione di spiegazioni alternative di un fenomeno o di una determinata situazione e nella valutazione di tutti i fattori che minano la validità delle ipotesi formulate. Prevede varie fasi in cui: si individuano le ipotesi astrattamente in grado di spiegare le dinamiche osservate ed i dati a favore e contro ciascuna di esse; si incrociano le ipotesi con i dati disponibili e si analizza la valenza diagnostica dei dati (si identificano cioè quali tra questi sono più utili per valutare il grado di probabilità di ciascuna ipotesi); si stima la probabilità di realizzazione delle singole ipotesi, concentrandosi soprattutto sui fattori che militano contro tale probabilità; si analizza quanto le conclusioni raggiunte dipendano dalla veridicità dei dati posti a loro fondamento e si considerano i riflessi che sull’analisi avrebbe l’even-

tualità che quei dati si rivelassero erronei ovvero passibili di differente interpretazione; si identificano i profili da monitorare attraverso la **ricerca informativa** per verificare se gli eventi stanno assumendo un andamento diverso rispetto a quello ipotizzato.

ANALISI DEL RISCHIO

Metodo ampiamente impiegato in ambito economico e tecnico, utilizzato anche dall'intelligence con riguardo alla sicurezza nazionale. In tal caso, consiste nell'individuazione e valutazione delle vulnerabilità, delle minacce e del loro potenziale impatto tanto con riferimento a contesti geografici o fenomeni quanto in relazione all'ambito delle informazioni classificate, ai fini dell'adozione delle necessarie contromisure.

ANALISI SWOT

Metodo di analisi impiegato per valutare i punti di forza (*Strengths*) e di debolezza (*Weaknesses*), le opportunità (*Opportunities*) e le minacce (*Threats*) di un progetto o di una situazione. Il vaglio, in tal modo effettuato, di fattori interni (punti di forza e debolezza) ed esterni (opportunità e minacce) permette di definire un quadro completo, utile per prendere decisioni in grado di valorizzare i profili "positivi" e di mitigare o, ove possibile, annullare i profili "negativi".

ANALISTA

Appartenente ad un **organismo informativo** specializzato nell'attività di **analisi**. Si avvale di una serie di metodologie (**analisi SWOT**, **analisi delle ipotesi confliggenti**, etc.),

procedendo ad integrare le informazioni con il quadro conoscitivo derivante dal **patrimonio informativo** sul fatto o sul fenomeno in esame, ad enucleare gli elementi di novità e gli aspetti pregnanti e ad elaborare **prodotti intelligence** di taglio situazionale e previsionale, facendo perno tanto su una preparazione specialistica quanto su una spiccata attitudine al ragionamento deduttivo ed induttivo.

ANS

Vedi **AUTORITÀ NAZIONALE PER LA SICUREZZA**

ANTENNA

In gergo indica:

- a) un appartenente ad un servizio di informazione che opera stabilmente in un contesto informativo di interesse dove non esistono articolazioni periferiche dell'agenzia intelligence di appartenenza;
- b) un appartenente ad un servizio di informazione cui sono affidati compiti di collegamento con strutture o enti esterni.

APPOSIZIONE DEL SEGRETO DI STATO

Provvedimento con cui il Presidente del Consiglio dei ministri dispone che siano coperti da **segreto di Stato** atti, documenti, notizie, attività od ogni altra cosa la cui diffusione sia idonea a recare danno agli interessi supremi dello Stato.

AREA CONTROLLATA

In tema di tutela della sicurezza delle informazioni, è l'area, predisposta in prossimità di un'**area riservata**, ove posso-

no essere trattate solo informazioni classificate a livello RISERVATO. Deve essere dotata di misure di protezione tali da consentire l'accesso alle sole persone autorizzate per motivi attinenti al loro impiego, incarico o professione.

AREA DI INTERESSE

Area geografica o tematica di interesse per la sicurezza nazionale.

AREA RISERVATA

In tema di tutela della sicurezza delle informazioni, è l'area dove vengono trattate informazioni con classifica di segretezza superiore a RISERVATO. Sottoposta a vigilanza, deve essere dotata di specifiche misure di protezione, atte a limitare l'accesso al solo personale autorizzato, e di sistemi anti-intrusione.

ATTENDIBILITÀ

Termine impiegato per indicare tanto il livello di affidabilità di una **fonte** quanto il grado di fondatezza di una **notizia**.

Vedi anche **VALUTAZIONE**

ATTIVITÀ DI INFORMAZIONE PER LA SICUREZZA

L'insieme delle attività di **ricerca informativa**, **elaborazione** e **disseminazione** di informazioni svolte al fine di prevenire, rilevare, contenere e contrastare le minacce alla **sicurezza nazionale**. Tali attività, sommariamente schematizzate nel **ciclo intelligence**, in ambito nazionale sono affidate in via esclusiva al Dipartimento delle informazioni per la sicurezza, all'Agenzia informazioni e sicurezza

esterna ed all’Agenzia informazioni e sicurezza interna che le svolgono, in base alle rispettive competenze, fornendo continuativo supporto alle Autorità di governo responsabili della sicurezza dello Stato ed interagendo con le Forze di polizia ed ulteriori interlocutori istituzionali, inclusi i servizi collegati.

Oltre all’espressione utilizzata dal Legislatore, è diffuso l’uso della locuzione “attività intelligence”.

ATTIVITÀ ECONOMICHE SIMULATE

Iniziative economiche finalizzate a “coprire” attività di **ricerca informativa**. L’uso di tale **strumento operativo** da parte dell’Agenzia informazioni e sicurezza esterna e dell’Agenzia informazioni e sicurezza interna viene autorizzato dal Direttore generale del Dipartimento delle informazioni per la sicurezza, previa comunicazione al Presidente del Consiglio dei ministri o all’Autorità delegata, ove istituita.

ATTIVITÀ INFO-OPERATIVA

Insieme delle attività condotte mediante fiduciari ovvero direttamente dagli appartenenti ai servizi di informazione avvalendosi degli **strumenti operativi**.

ATTIVITÀ INFORMATIVA

Termine colloquiale impiegato per indicare l’**attività di informazione per la sicurezza**.

ATTIVITÀ INTELLIGENCE

Vedi **ATTIVITÀ DI INFORMAZIONE PER LA SICUREZZA**

AUTENTICAZIONE

Verifica dell'identità o di altre caratteristiche di un utente, di un dispositivo o di una procedura ovvero dell'originatore e dell'integrità dei dati. Costituisce spesso una condizione per accedere ai sistemi informativi e di comunicazione. A tal fine vengono frequentemente impiegati metodi che associano vari strumenti di riconoscimento, quali dati biometrici, tesserini identificativi, password, etc.

AUTORITÀ DELEGATA

Il Ministro senza portafoglio o il Sottosegretario di Stato cui il Presidente del Consiglio dei ministri, esercitando una facoltà riservatagli dalla legge, abbia eventualmente delegato le funzioni che, in materia di **attività di informazione per la sicurezza**, non gli sono attribuite in via esclusiva. Informa costantemente il Presidente del Consiglio dei ministri sulle modalità di esercizio delle funzioni delegate. Fa parte del Comitato interministeriale per la sicurezza della Repubblica e non può svolgere ulteriori funzioni di governo.

AUTORITÀ NAZIONALE PER LA SICUREZZA (ANS)

È l'Autorità italiana – individuata dalla legge nel **Presidente del Consiglio dei ministri** – cui compete garantire la tutela amministrativa del **segreto di Stato** e delle informazioni classificate avvalendosi dell'**Organizzazione nazionale per la sicurezza**. In tale quadro, l'ANS tra l'altro determina gli indirizzi per la negoziazione e per l'attuazione degli accordi con gli altri stati e con gli organismi internazionali finalizzati alla tutela delle informazioni

classificate o coperte da segreto di Stato e dispone la proroga, nei casi previsti dalla legge, dell'efficacia del segreto di Stato e delle **classifiche di segretezza** oltre il termine di quindici anni.

AUTORIZZAZIONE ALL'ACCESSO CIFRA

Autorizzazione di durata quinquennale che, nell'ambito dell'**Organizzazione nazionale per la sicurezza**, consente alle persone fisiche di accedere a informazioni, materiali e documentazione **COMSEC**.

B

BONIFICA

Vedi VERIFICA AMBIENTALE

BRUCIARE/BRUCIATURA

Termine colloquiale impiegato per indicare la **compromissione** di un agente, di una fonte confidenziale o di una operazione.

C

CARATTERISTICHE DEI PRODOTTI INTELLIGENCE

Qualità che devono contraddistinguere i **prodotti intelligence**: accuratezza, attualità, completezza, concretezza, oggettività (assenza di preconcetti, influenze e condizionamenti), rilevanza (capacità di apportare conoscenze utili a migliorare la comprensione di una situazione) e tempestività.

CASE OFFICER

Vedi **GESTORE**

CAVEAT

Previsione che definisce i limiti entro cui una specifica attività può essere svolta. Ne costituiscono esempi le regole di ingaggio – dettate per stabilire ambito e finalità dell'attività intelligence nei teatri di crisi – e l'impiego di indicatori per circoscrivere la circolazione di informazioni. In Italia, tipica al riguardo è la dicitura Esclusivo Ambito Nazionale (E.A.N.) aggiunta alla classifica di segretezza per indicare che il documento su cui è apposta e le informazioni in esso contenute non sono destinati alla condivisione con organismi informativi o soggetti esteri.

CELLULA DORMIENTE

Soggetto integrato nel tessuto di un paese – ove tiene una condotta atta a non destare sospetti – che opera a favore

di un'agenzia intelligence estera o di un'organizzazione terroristica. Può essere attivato per azioni di natura offensiva (rispettivamente di tipo spionistico o terroristico) anche dopo molti anni dall'arrivo nel paese o dal suo reclutamento.

Laddove la cellula sia formata da più individui, questi sovente non si conoscono fra loro, per ridurre al minimo i rischi di smantellamento dell'intera rete in caso di arresto o scoperta di un componente.

CENTRO

- a) Articolazione periferica dell'Agenzia informazioni e sicurezza esterna o dell'Agenzia informazioni e sicurezza interna.
- b) Nella terminologia **COMSEC**, è l'area riservata nella quale sono trattate informazioni o materiali classificati COMSEC. I centri COMSEC in cui si provvede alla ricezione e trasmissione di comunicazioni protette assumono la denominazione di "centri comunicazioni classificate".

CENTRO DI VALUTAZIONE

Organismo, accreditato dall'**Autorità Nazionale per la Sicurezza**, responsabile di valutare la conformità di un prodotto o di un sistema informatico ai requisiti di sicurezza richiesti per la trattazione di materiale classificato.

CERTIFICAZIONE

In materia di sicurezza informatica, è l'attestazione da parte dell'**ente di certificazione** dell'idoneità di un prodotto o di un sistema a garantire i requisiti di sicurezza richiesti.

CICLO INTELLIGENCE

Termine che descrive il complesso delle fasi in cui si articola l'**attività di informazione per la sicurezza**, dalle indicazioni delle Autorità di governo fino alla disseminazione di **prodotti intelligence** ai fruitori istituzionali, passando per **pianificazione informativa, ricerca informativa** ed **elaborazione**.

Generalmente non inclusa nelle rappresentazioni grafiche del ciclo intelligence, ma di grande rilevanza, la fase di *feedback* in cui si valuta in che misura i prodotti intelligence abbiano soddisfatto le esigenze conoscitive delle Autorità di governo e degli altri interlocutori istituzionali in materia di sicurezza nazionale e si determina se, su una specifica situazione o fenomeno, siano necessarie ulteriori attività di ricerca ed elaborazione. L'esigenza di colmare eventuali lacune conoscitive riavviando la fase della ricerca informativa può essere segnalata anche dagli analisti, e dunque prima che il ciclo intelligence, nella sua forma astratta, sia stato completato.

CIFRA

- a) Codice o algoritmo che consente di rendere inintelligibili testo o dati e di riportarli in chiaro.
- b) In ambito **COMSEC**, indicazione apposta sui materiali e sulla documentazione contenenti elementi crittografici per la cifratura di informazioni classificate.

CIFRATURA

Vedi **CODIFICA**

CISR

Vedi **COMITATO INTERMINISTERIALE PER LA SICUREZZA DELLA REPUBBLICA**

CLASSIFICA DI SEGRETEZZA

Indicatore del livello di segretezza attribuito in ambito nazionale ad informazioni la cui conoscenza non autorizzata sia idonea a recare pregiudizio agli interessi fondamentali della Repubblica. L'ordinamento italiano prevede, in ordine decrescente di potenziale danno, le classifiche **SEGRETISSIMO (SS)**, **SEGRETO (S)**, **RISERVATISSIMO (RR)**, **RISERVATO (R)**, sanzionando penalmente le violazioni in materia. Le classifiche: limitano l'**accesso** alle informazioni classificate, e conseguentemente la loro circolazione, alle sole persone che hanno necessità di conoscerle in funzione del proprio incarico e sono altresì in possesso del **Nulla Osta di Sicurezza** per le informazioni con classifica superiore a **RISERVATO**; impongono l'adozione di un sistema di misure, proporzionate alla rilevanza dell'interesse tutelato, intese ad assicurare l'effettività della limitazione e la protezione delle informazioni classificate.

Spesso sovrapposte, nell'immaginario collettivo, al **segreto di Stato**, sono in realtà da esso nettamente distinte per disciplina ed effetti, inclusi quelli che riguardano il processo penale: le classifiche di segretezza, infatti, non precludono all'Autorità giudiziaria la possibilità di acquisire documenti classificati, ma la vincolano a curarne la conservazione con modalità che ne tutelino la riservatezza, garantendo il diritto delle parti del procedimento a prenderne visione.

Vedi anche **DECLASSIFICA**, **CLASSIFICHE DI SEGRETEZZA INTERNAZIONALI E COMUNITARIE** e **NECESSITÀ DI CONOSCERE**

CLASSIFICAZIONE

Processo consistente nel determinare quali informazioni siano meritevoli di tutela e nel rendere tale caratteristica riconoscibile attraverso l'apposizione di una **classifica di segretezza**. Il relativo potere compete ai soggetti che formano il documento, l'atto o lo acquisiscono, ovvero sono responsabili della cosa nonché, nell'ambito della Pubblica amministrazione, ai superiori gerarchici e alle autorità di vertice.

CLASSIFICHE DI SEGRETEZZA INTERNAZIONALI E COMUNITARIE

Classifiche di segretezza previste da trattati, convenzioni, accordi, regolamenti, etc. recepiti nell'ordinamento italiano o cui sia data attuazione in conformità alle norme vigenti. In ambito NATO e UE vigono le seguenti classifiche di segretezza: TRÈS SECRET/TOP SECRET, SECRET/SECRET, CONFIDENTIEL/CONFIDENTIAL, RESTREINT/RESTRICTED, rispettivamente corrispondenti alle classifiche nazionali SEGRETISSIMO, SEGRETO, RISERVATISSIMO, RISERVATO. Nella pratica si associano alla **qualifica di sicurezza**.

CLAUSOLA CATCH-ALL

Nell'ambito della **controproliferazione**, clausola che permette di assoggettare al regime autorizzatorio dell'Autorità di governo beni a duplice uso (cd. "**materiali dual use**") che non rientrano tra quelli già individuati dalla normativa di settore.

CODIFICA

Operazione consistente nel rendere inintelligibili testo o dati attraverso l'impiego di una **cifra**.

Vedi CRITTANALISI, CRITTOGRAFIA e CRITTOLOGIA

COLLABORAZIONE INTERNAZIONALE INTELLIGENCE

Il complesso dei rapporti sviluppati con **servizi collegati** al fine di arricchire il patrimonio informativo e di incrementare le capacità operative e di analisi attraverso l'affinamento delle cognizioni e delle tecniche utilizzate nell'attività di informazione per la sicurezza.

Si attua su base bilaterale ovvero multilaterale, mediante la partecipazione a esercizi dedicati o a comitati e gruppi di lavoro intelligence inseriti in ambiti di collaborazione più ampi.

Vedi anche COOPERAZIONE INTERNAZIONALE INTELLIGENCE

COLLABORAZIONE ISTITUZIONALE

Dovere di collaborare con l'Agenzia informazioni e sicurezza esterna e l'Agenzia informazioni e sicurezza interna ai fini dell'**attività di informazione per la sicurezza** stabilito da previsioni di legge per Forze armate e Forze di polizia. Analoga collaborazione a favore degli organismi informativi, per quanto riguarda l'accesso agli archivi informatici, è prevista anche per i soggetti pubblici e privati erogatori di servizi di pubblica utilità. Specifiche disposizioni prevedono e disciplinano un rapporto di collaborazione degli organismi informativi con l'Autorità giudiziaria nonché con le pubbliche amministrazioni e gli altri soggetti, anche privati, interessati all'acquisizione di informazioni per la sicurezza, per esempio in materia cibernetica.

COLLAZIONE

Fase dell'**elaborazione** in cui si raggruppano e si raffinano le acquisizioni informative.

COLLEGATO ESTERO

Vedi **SERVIZIO COLLEGATO**

COMINT (COMMUNICATIONS INTELLIGENCE)

Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale provenienti da segnali emessi da sistemi elettromagnetici esteri di comunicazione. È una sottocategoria della **SIGINT**.
Vedi anche **CRITTANALISI**

COMITATO DI ANALISI STRATEGICA ANTITERRORISMO (CASA)

Tavolo permanente tra Forze di polizia e servizi di informazione per la condivisione e valutazione delle informazioni relative alla minaccia terroristica interna ed internazionale. Costituito all'indomani dell'11 settembre 2001, opera presso il Ministero dell'Interno.

COMITATO DI SICUREZZA FINANZIARIA (CSF)

Organismo costituito all'indomani dell'11 settembre 2001 con il compito di contrastare il terrorismo internazionale, specie per quanto riguarda le attività di finanziamento. Nel 2007 il suo mandato è stato esteso alla lotta contro il riciclaggio dei proventi di attività criminose. Presieduto dal Direttore generale del Tesoro ed incaricato, tra l'altro, di monitorare il sistema sanzionatorio internazionale, si avvale anche del contributo informativo dell'Agenzia informazioni e sicurezza esterna e dell'Agenzia informazioni e sicurezza interna.

COMITATO INTERMINISTERIALE PER LA SICUREZZA DELLA REPUBBLICA (CISR)

Organo collegiale del Sistema di informazioni per la sicurezza della Repubblica con funzioni di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza. È l'organismo al quale, tra l'altro, compete definire, su base annuale, gli **obiettivi informativi** su cui concentrare l'**attività di informazione per la sicurezza** e deliberare sulla ripartizione delle risorse finanziarie tra il Dipartimento delle informazioni per la sicurezza e i servizi di informazione nonché sui relativi bilanci. È presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, ove istituita, e dai Ministri degli affari esteri, dell'interno, della difesa, della giustizia, dell'economia e finanze e dello sviluppo economico. Le funzioni di segretario sono svolte dal Direttore generale del Dipartimento delle informazioni per la sicurezza.

COMITATO PARLAMENTARE PER LA SICUREZZA DELLA REPUBBLICA (COPASIR)

Organo bicamerale, composto da 5 senatori e 5 deputati e presieduto da un esponente dell'opposizione, con funzioni consultive e di **controllo sul Sistema di informazione per la sicurezza della Repubblica**. A tal fine tra l'altro: riceve una **relazione sull'attività dei servizi di informazione** ed una serie di comunicazioni in materia, ad esempio, di gestione finanziaria degli organismi informativi, utilizzo delle **garanzie funzionali** e conferma dell'opposizione del **segreto di Stato**; svolge periodiche audizioni dei vertici politici del Sistema di informazione per la sicurezza della Repubblica (Presidente del Consiglio dei ministri e Autorità

delegata, ove istituita) e di quelli tecnici (Direttore generale del Dipartimento delle informazioni per la sicurezza e Direttori dell'Agazia informazioni e sicurezza esterna e dell'Agazia informazioni e sicurezza interna); può audire elementi esterni in grado di fornire informazioni utili e, in casi eccezionali, personale degli organismi informativi (salvo che il Presidente del Consiglio dei ministri non si opponga); può accedere alle strutture del Sistema di informazione per la sicurezza della Repubblica (salvo richieste di differimento temporale del Presidente del Consiglio dei ministri); esprime il proprio parere sui provvedimenti normativi previsti dalla legge 124/2007, sulle delibere assunte dal CISR in merito alla ripartizione delle risorse finanziarie tra gli organismi informativi e sui relativi bilanci, nonché sul piano annuale delle attività dell'Ufficio ispettivo. È preventivamente informato delle nomine dei vertici degli organismi informativi. Qualora riscontri violazioni, informa il Presidente del Consiglio dei ministri e riferisce ai Presidenti delle Camere; può richiedere al Presidente del Consiglio dei ministri di disporre inchieste interne volte a verificare la correttezza delle condotte di appartenenti o ex appartenenti agli organismi di informazione. Il COPASIR è tenuto a riferire al Parlamento sulla propria attività con una relazione annuale e può trasmettere alle Camere informative o relazioni urgenti.

COMPARTIMENTAZIONE

Modalità organizzativa tradizionalmente adottata dagli organismi informativi in base alla quale, tanto all'esterno che all'interno, l'accesso alle notizie su personale, assetti ed attività è regolato dal principio della **necessità di conoscere**.

COMPARTO INFORMATIVO/INTELLIGENCE

Vedi **COMUNITÀ INTELLIGENCE** e **SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA**

COMPROMISSIONE

Disvelamento, intenzionale o fortuito, di un'informazione, un'operazione, un agente o una fonte. Nel caso di informazioni classificate, si verifica allorquando queste vengono in qualsiasi modo rivelate a persona non autorizzata ovvero non in possesso di adeguata **abilitazione di sicurezza** o che non abbia la **necessità di conoscere**.

COMPUSEC (COMPUTER SECURITY)

Misure di sicurezza finalizzate a prevenire la deliberata o accidentale acquisizione, modifica o distruzione delle informazioni classificate o coperte da segreto di Stato, memorizzate o elaborate da sistemi informativi e l'uso non autorizzato di tali sistemi.

Vedi anche **TEMPEST**

COMSEC (COMMUNICATIONS SECURITY)

Insieme delle misure di sicurezza (incluse quelle di natura crittografica) finalizzate a tutelare le informazioni classificate o coperte da segreto di Stato trattate con sistemi di comunicazione e trasmissione dati.

Vedi anche **TEMPEST**

COMUNICAZIONE ISTITUZIONALE

Attività volta a stabilire con l'opinione pubblica un rapporto di trasparenza, pur nel rispetto della riservatezza che necessariamente contraddistingue il comparto intelligence. Introdotta dalla legge 124/2007 – che la ha affidata al Dipar-

timento delle informazioni per la sicurezza – si esplicita in iniziative finalizzate a far conoscere, anche attraverso un sito web dedicato, i compiti degli organismi informativi nonché le linee essenziali dell'organizzazione e dell'attività. Vedi anche **CULTURA DELLA SICUREZZA**

COMUNITÀ INTELLIGENCE

Il complesso degli organismi informativi di un Paese incaricati, in base alle rispettive legislazioni, di svolgere **attività di informazione per la sicurezza**. In ambito nazionale è costituita dal Dipartimento delle informazioni per la sicurezza, dall'Agenzia informazioni e sicurezza esterna e dall'Agenzia informazioni e sicurezza interna. Vedi anche **SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA**

CONFIDENTE

Vedi **FONTE CONFIDENZIALE**

CONSIGLIO GENERALE PER LA LOTTA ALLA CRIMINALITÀ ORGANIZZATA

Organo presieduto dal Ministro dell'Interno, di cui fanno parte i vertici delle Forze di Polizia, della Direzione Investigativa Antimafia e dei servizi di informazione. Ha il compito di elaborare linee guida per le attività investigative e di prevenzione anticrimine, nonché in materia di coordinamento e razionalizzazione delle risorse.

CONTROINDICAZIONI

Elementi informativi suscettibili di influire negativamente sulla valutazione dell'**affidabilità** di un soggetto

o di un operatore economico in possesso di **abilitazione di sicurezza** (nel qual caso possono determinarne la sospensione o la revoca) o per cui sia in corso il procedimento per il rilascio dell'abilitazione stessa (nel qual caso possono causare il diniego).

Si utilizza anche l'espressione soggetto o paese controindicato per evidenziarne la pericolosità per la sicurezza nazionale.

CONTROINFORMAZIONE

Diffusione di informazioni in violazione di embarghi o censure adottati da regimi autoritari.

CONTROINGERENZA

Attività volta a prevenire, rilevare, contenere, contrastare ed, eventualmente, sfruttare a proprio vantaggio la penetrazione in ambiti istituzionali e comparti strategici del Paese condotta da attori, statuali e non, al fine di orientare in senso lesivo per la sicurezza nazionale processi decisionali e conseguenti condotte in campo politico, militare, economico-finanziario ed industriale. È una delle componenti della **counterintelligence**.

Vedi anche **INGERENZA**

CONTROLLO SUL SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA

Complesso delle attività poste in essere da organi e autorità individuati dalla legge al fine di verificare che l'azione del Sistema di informazione per la sicurezza della Repubblica avvenga nel rispetto della Costituzione e delle leggi, nell'esclusivo interesse e per la difesa della Repub-

blica e delle sue istituzioni. Il controllo parlamentare è esercitato dal **Comitato parlamentare per la sicurezza della Repubblica**. Il controllo di legittimità sugli atti del Sistema e quello amministrativo-contabile sulle procedure afferenti il suo bilancio autonomo (con riferimento esclusivo alle spese ordinarie) sono svolti rispettivamente dalla Corte dei Conti e dall'Ufficio di Bilancio e Ragioneria della Presidenza del Consiglio dei ministri, tramite loro uffici distaccati presso il Dipartimento delle informazioni per la sicurezza.

Compiti di controllo sono affidati anche ad organi incaricati nel Dipartimento delle informazioni per la sicurezza: l'Ufficio Centrale Ispettivo, per ciò che concerne la verifica della conformità alle leggi, ai regolamenti, alle direttive e alle disposizioni del Presidente del Consiglio dei ministri dell'attività dei servizi di informazione; l'Ufficio Centrale degli Archivi, in relazione alla vigilanza sulla sicurezza, sulla tenuta e sulla gestione degli archivi degli organismi informativi; l'Organo di Controllo Interno, per quanto riguarda il monitoraggio della spesa.

CONTROPROLIFERAZIONE

Attività volta a prevenire, rilevare e contrastare la realizzazione di armi di distruzione di massa (ordigni nucleari, armi chimiche, biologiche e radiologiche e correlati vettori). Include le iniziative tese ad individuare il traffico dei materiali connessi e di quelli cd. *"dual use"*, nonché di tecnologie e *know-how*.

CONTROPROPAGANDA

Attività volta a rilevare e contrastare le azioni di propaganda svolte da attori ostili. Comprende le iniziative fina-

lizzate a neutralizzare o mitigare gli effetti della propaganda avversaria ovvero a sfruttarla a proprio vantaggio.

CONTROSPIONAGGIO

Attività difensiva volta a prevenire, rilevare, contenere e contrastare le azioni di **spionaggio** condotte da agenzie intelligence straniere nonché da individui od organizzazioni operanti in modo autonomo ovvero in collegamento con servizi di informazione esteri.

A seconda dei casi, si traduce in iniziative:

- tese a creare un'adeguata cornice di sicurezza attorno agli obiettivi oggetto di aggressione spionistica;
- miranti al reclutamento del soggetto che conduce attività di spionaggio;
- repressive, con le quali si interrompe l'attività spionistica attraverso l'adozione di misure di natura diplomatica (tipica, in questo contesto, è la dichiarazione di una spia accreditata presso una rappresentanza diplomatica estera come "*persona non grata*" - PNG), amministrativa (rifiuto/revoca del visto) o giudiziaria (arresto);
- disinformative, mediante le quali l'apparato di controspionaggio sfrutta a proprio vantaggio la spia avversaria consentendole di acquisire, eventualmente grazie alla collaborazione di una **fonte confidenziale**, notizie false o artatamente distorte (vedi anche **INTOSSICAZIONE**).

Il reclutamento di spie avversarie e le manovre disinformative costituiscono uno dei tratti tipici del controspionaggio (in gergo spesso indicato con il solo acronimo, CS), che si caratterizza proprio poiché l'azione di contenimento/contrasto della minaccia mira, ove possibile, a trasformare in opportunità una condotta lesiva per la sicurezza nazionale, sfruttando a proprio vantaggio una rete spio-

nistica avversaria. È una delle componenti della **counter-intelligence**.

Nell'ambito del Sistema di informazione per la sicurezza della Repubblica, l'attività è svolta dall'Agenzia informazioni e sicurezza interna in territorio nazionale e dall'Agenzia informazioni e sicurezza esterna all'estero.

CONTROTERRORISMO

Attività volta a prevenire, rilevare, contenere e contrastare le condotte di natura terroristica, ivi incluse quelle di carattere prodromico e/o strumentale. Comprende le iniziative tese a monitorare i contesti eversivo-terroristici, disarticolare gruppi e cellule, inibire le pianificazioni offensive di sodalizi e singoli individui e contrastarne le attività di propaganda, indottrinamento e reclutamento. Vedi anche **MINACCIA TERRORISTICA**

COOPERAZIONE INTERNAZIONALE INTELLIGENCE

Spesso impiegato come sinonimo di **collaborazione internazionale intelligence**, in un'accezione tecnica indica una interazione di tipo operativo con un **servizio collegato**. Vedi anche **ACCORDO DI COOPERAZIONE/COLLABORAZIONE**

COORDINAMENTO

Attività di pianificazione, raccordo e razionalizzazione svolta dal **Presidente del Consiglio dei ministri** a livello politico e dal **Dipartimento delle informazioni per la sicurezza** a livello amministrativo e tecnico-operativo, per garantire piena unitarietà all'**attività di informazione per la sicurezza**. Compete ad esempio al Dipartimento delle informazioni per la sicurezza assicurare il necessario rac-

cordo info-operativo tra i servizi di informazione, nei casi in cui l'Agazia informazioni e sicurezza esterna e l'Agazia informazioni e sicurezza interna operino al di fuori dell'ambito territoriale di rispettiva competenza.

COPASIR

Vedi **COMITATO PARLAMENTARE PER LA SICUREZZA DELLA REPUBBLICA**

COPERTURA

Misure necessarie a proteggere persone, piani, operazioni, strutture o installazioni da attività intelligence ostile o rispetto a possibile **compromissione**.

Vedi anche **OPERAZIONE SOTTO COPERTURA**

COPERTURA INFORMATIVA

Capacità di un servizio di informazione di fornire ai fruitori istituzionali elementi conoscitivi utili ai fini della sicurezza nazionale su ambiti tematici, fenomeni, eventi, aree geografiche e soggetti/organizzazioni.

COUNTERINTELLIGENCE

Attività volta a prevenire, rilevare, contenere, contrastare ed, eventualmente, sfruttare a proprio vantaggio le iniziative intelligence condotte in danno della sicurezza nazionale da Stati e servizi di informazione esteri ovvero da individui e gruppi. **Controingerenza** e **controspionaggio** rappresentano le due componenti principali della counterintelligence che, peraltro, non si esaurisce in queste, includendo anche la controinfluenza e le azioni dirette a proteggere il comparto informativo nazionale da pene-

trazioni ostili, nonché quelle che mirano a preservare funzione e processo informativi rispetto a manipolazioni ed interferenze.

CRIMINALITÀ ORGANIZZATA

Fenomeno delinquenziale di natura associativa in grado anche di alterare le dinamiche politico-sociali ed economico-finanziarie di un paese e/o di un'area geografica ovvero, nei casi più gravi, di minacciare la stabilità internazionale.

CRITTANALISI

Principi e metodi necessari per rendere intellegibili, riportandoli alla loro versione originaria (cd. "in chiaro"), testo o dati cifrati, forzandone la **cifra**. È impiegata anche per testare la sicurezza del proprio codice, individuandone le vulnerabilità. Insieme alla **crittografia** – di cui rappresenta l'opposto speculare – forma la **crittologia**.

CRITTOGRAFIA

Principi e metodi necessari per assicurare la **codifica** e **decodifica** di testo o dati. Il termine è non di rado impiegato come sinonimo di **crittologia**.

CRITTOLOGIA

Disciplina scientifica che studia principi e metodi delle comunicazioni criptate, dissimulate e nascoste. Storicamente associata ai contesti militari ed intelligence e focalizzata sulla confidenzialità delle comunicazioni, ha conosciuto nuovi e notevoli sviluppi, dottrinari ed applicativi, in connessione con la crescita della digitalizzazione della

società contemporanea, ampliando i propri obiettivi alla integrità delle informazioni ed alla loro autenticazione. Include la **crittografia**, la **crittanalisi** e la **steganografia**.

CULTURA DELLA SICUREZZA

Conoscenza delle minacce alla sicurezza nazionale e delle connesse attribuzioni degli organismi informativi. Per rispondere ad un'avvertita esigenza in materia, il Legislatore italiano ha introdotto uno specifico compito istituzionale, affidando le attività di promozione e diffusione della cultura della sicurezza al Dipartimento delle informazioni per la sicurezza. Rientrano in tale ambito le iniziative volte a sviluppare una fattiva interlocuzione con il mondo accademico, le imprese ed i *media* in vista della instaurazione di una costruttiva sinergia tra comparto informativo e società civile a tutela della sicurezza nazionale.

CURRENT INTELLIGENCE

Informazioni di taglio situazionale su ambiti tematici, fenomeni, eventi, aree geografiche e soggetti/organizzazioni. Laddove soggette a perdere rapidamente attualità e rilevanza, vengono tempestivamente disseminate ai fruitori istituzionali.

CYBER-DEFENCE

L'insieme della dottrina, dell'organizzazione e delle attività volte a prevenire, rilevare, limitare e contrastare gli effetti degli attacchi condotti nel e tramite il *cyber-space* ovvero in danno di uno o più dei suoi elementi costitutivi.

CYBER-INTELLIGENCE

Ricerca ed elaborazione di notizie di interesse nel e sul *cyber-space* al fine di prevenire, rilevare, contenere e contrastare le minacce alla sicurezza nazionale, con riguardo ad esempio alle infrastrutture critiche.

CYBER-SECURITY

Condizione in cui il *cyber-space* risulti protetto rispetto ad eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittime ovvero nel blocco dei sistemi informativi, grazie ad idonee misure di sicurezza fisica, logica e procedurale. Queste includono: *audit* di sicurezza, gestione di aggiornamenti (*patches*) di sicurezza, procedure di autenticazione, gestione degli accessi, analisi del rischio, rilevazione e reazione ad incidenti/attacchi, mitigazione degli impatti, recupero delle componenti oggetto di attacco, addestramento e formazione del personale, nonché verifica e potenziamento della sicurezza fisica dei locali dove sono collocati i sistemi informativi e di comunicazione.

CYBER-SPACE

L'insieme delle infrastrutture informatiche interconnesse, comprensivo di *hardware*, *software*, dati ed utenti nonché delle relazioni logiche, comunque stabilite, tra di essi. Include tra l'altro internet, reti di comunicazione, sistemi attuatori di processo ed apparecchiature mobili dotate di connessione di rete.

CYBER-THREAT

Vedi MINACCIA CIBERNETICA

CYBER-WAR

L'insieme delle operazioni condotte nel e tramite il *cyber-space* al fine di negare all'avversario – statuale o non – l'uso efficace di sistemi, armi e strumenti informatici o comunque di infrastrutture e processi da questi controllati. Include anche attività di difesa e "capacitanti" (volte cioè a garantirsi la disponibilità e l'uso del *cyber-space*). Può assumere la fisionomia di un conflitto di tipo "tradizionale" – quando coinvolge le forze armate di due o più stati – ovvero "irregolare", quando si svolge tra forze ufficiali e non ufficiali. Può rappresentare l'unica forma di confronto ovvero costituire uno degli aspetti di un conflitto che coinvolga altri domini (terra, mare, cielo e spazio); in entrambi i casi, i suoi effetti possono essere limitati al *cyber-space* ovvero tradursi in danni concreti, inclusa la perdita di vite umane.

D

D

DECIFRATURA

Vedi **DECODIFICA**

DECLASSIFICA

Riduzione ad un livello inferiore o eliminazione della **classifica di segretezza**.

Il termine italiano risulta onnicomprensivo rispetto al mondo anglosassone, che distingue tra riduzione (*downgrading*) e rimozione (*declassification*) della classifica di segretezza. La legge 124/2007 ha introdotto un meccanismo in base al quale la classifica di segretezza viene automaticamente ridotta al livello inferiore (per esempio, da **RISERVATISSIMO** a **RISERVATO**) trascorsi cinque anni dalla data della sua apposizione; dopo ulteriori cinque anni cessa ogni vincolo di classifica. Tali automatismi non si applicano quando i termini di efficacia del vincolo sono prorogati con provvedimento motivato dall'ente che ha apposto la classifica o, nel caso di proroga superiore ai quindici anni, dal Presidente del Consiglio dei ministri.

DECODIFICA

Operazione che consente al destinatario di un messaggio cifrato di ricostruirne il testo in chiaro. È l'operazione inversa alla **codifica**.

Vedi anche **CRITTOGRAFIA**

DECRIPTAZIONE

Operazione consistente nella forzatura del codice dei messaggi cifrati.

Vedi anche **CRITTANALISI**

DEQUALIFICA

Eliminazione della **qualifica di sicurezza**. Deve avvenire con il consenso dell'originatore.

DIPARTIMENTO DELLE INFORMAZIONI PER LA SICUREZZA (DIS)

Organismo del Sistema di informazione per la sicurezza della Repubblica del quale si avvalgono il Presidente del Consiglio dei ministri e l'Autorità delegata, ove istituita, al fine di assicurare piena unitarietà all'**attività di informazione per la sicurezza**.

In tale ottica il DIS, titolare di competenze esclusive in materia di analisi strategica, formazione, **comunicazione istituzionale** e promozione della **cultura della sicurezza**: coordina l'attività dei servizi di informazione, verificandone i risultati ed evitando duplicazioni e sovrapposizioni nella ricerca informativa; assicura il raccordo del flusso informativo diretto all'Autorità politica ed agli altri enti istituzionali, promuovendo altresì lo scambio informativo con le amministrazioni aventi compiti contigui a quelli del Sistema; garantisce unitarietà di indirizzo in materia di politiche del personale e gestisce unitariamente approvvigionamenti e servizi logistici del comparto informativo; esercita talune funzioni di controllo sulle attività del comparto informativo (vedi anche **CONTROLLO SUL SISTEMA DI INFORMAZIONE PER LA SICUREZZA**

DELLA REPUBBLICA) e svolge attività in materia di tutela amministrativa del **segreto di Stato** e delle informazioni classificate. Compete, tra l'altro, al Direttore generale del DIS – nominato dal Presidente del Consiglio dei ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica – autorizzare l'esercizio di attività economiche simulate e l'uso di identità di copertura nonché, quale Organo nazionale di sicurezza, dirigere e coordinare l'**Organizzazione nazionale per la sicurezza**.

DIS

Vedi **DIPARTIMENTO DELLE INFORMAZIONI PER LA SICUREZZA**

DISCIPLINE INTELLIGENCE

Metodologie e prassi che guidano lo svolgimento dell'**attività di informazione per la sicurezza** e l'attuazione dei singoli passaggi in cui essa concretamente si articola in base alle risorse, tecniche e/o umane, impiegate. Sono le cd. "INT" del gergo intelligence, quali, ad esempio, la **HUMINT**, la **SIGINT**, l'**OSINT**, etc. La specificità delle fonti da cui provengono le notizie conferisce a ciascuna disciplina tratti caratteristici relativi tanto alla **ricerca informativa** che all'**elaborazione**.

DISINFORMAZIONE

Diffusione di notizie infondate o artatamente distorte al fine di danneggiare l'immagine pubblica di un avversario e/o di influenzarne le scelte.

Vedi anche **INFORMATION WARFARE**, **INTOSSICAZIONE** e **PSYOPS**

DISPOSITIVO DI RICERCA

Complesso di risorse e **strumenti operativi** impiegati nella **ricerca informativa**.

DISSEMINAZIONE

Inoltre ai fruitori istituzionali di informazioni di interesse per la sicurezza nazionale.

Vedi **CICLO INTELLIGENCE** e **PRODOTTI INTELLIGENCE**

DOCUMENTI DI COPERTURA

Vedi **IDENTITÀ DI COPERTURA**

DOCUMENTO CLASSIFICATO

Qualsiasi supporto (materiale o immateriale, analogico o digitale) contenente informazioni classificate e, pertanto, sottoposto a misure di protezione fisica, logica e tecnica dall'atto della sua originazione a quello della sua distruzione o declassifica; durante tale "arco di vita" specifiche modalità ne disciplinano gestione e trattazione. Le singole parti di un documento possono richiedere classifiche differenti; in questo caso il livello generale di classifica dell'intero documento è pari almeno a quello della parte con classifica più elevata.

Vedi anche **CLASSIFICA DI SEGRETEZZA**

E

E

ELABORAZIONE

Il complesso delle attività (tecniche, logico-concettuali, etc.) volte a trasformare le **notizie** acquisite attraverso la ricerca informativa in **informazioni** utili ai fini della tutela della sicurezza nazionale. In tale ampia accezione, si riferisce sia alle attività di “processamento” di base (traduzione, trascrizione, decrittazione, etc.) – di complessità e tecnicismo variabili a seconda della natura della fonte da cui proviene la notizia – sia alla verifica dell’attendibilità e alla **collazione**, sia all’**analisi** che alla **produzione**. A titolo esemplificativo, acquisita attraverso intercettazione una notizia relativa ad una minaccia di attentato terroristico in Italia, questa verrà tradotta – se in lingua estera – e trascritta, valutata in termini di attendibilità (per escluderne, ad esempio, l’assoluta infondatezza) e quindi trasmessa con carattere di urgenza alle Forze di polizia per gli aspetti di diretta ed immediata competenza e agli **analisti**, che potranno utilizzarla per realizzare prodotti intelligence situazionali o previsionali.

Vedi anche **CICLO INTELLIGENCE**

ELINT (ELECTRONIC INTELLIGENCE)

Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale provenienti da emissioni elettromagnetiche estere diverse dalle comunicazioni (per esempio, emissioni radar). È una sottocategoria della **SIGINT**.

ENTE DI CERTIFICAZIONE

Organismo responsabile della **certificazione** dei prodotti e dei sistemi informatici, dell'accreditamento dei **centri di valutazione**, nonché della definizione ed aggiornamento delle norme in tema di sicurezza delle tecnologie dell'informazione, ai fini della tutela delle informazioni classificate.

EVERSIONE

Fenomeno consistente nel tentativo di abbattere o sovvertire l'ordinamento costituzionale del Paese, attraverso condotte che possono andare dall'azione di propaganda agli atti terroristici.

F

FABBISOGNO INFORMATIVO

L'insieme delle informazioni di cui le Autorità di governo necessitano – quale supporto alle proprie decisioni in materia di sicurezza nazionale – per disporre di un esaustivo quadro conoscitivo su ambiti tematici, fenomeni, eventi, aree geografiche e soggetti/organizzazioni di interesse. Sulla base del fabbisogno di ciascun Ministro membro del Comitato interministeriale per la sicurezza della Repubblica vengono definiti annualmente gli **obiettivi informativi**.

FIDUCIARIO

Vedi **FONTE CONFIDENZIALE**

FONTE

Persona, cosa o sistema tecnologico da cui vengono ottenute/tratte notizie di interesse per la sicurezza nazionale. Vedi anche **FONTE APERTA**, **FONTE CHIUSA**, **FONTE CONFIDENZIALE**, **FONTE DOCUMENTALE** e **FONTE TECNICA**

FONTE APERTA

Fonte dalla quale è possibile e legittimo trarre notizie pubblicamente disponibili attraverso consultazione/osservazione diretta, su richiesta o previa sottoscrizione. La categoria delle fonti aperte comprende, per esempio, i mezzi di comunicazione di massa (radio e televisione, giornali e riviste, internet), le pubblicazioni ufficiali (governative o meno), le altre fonti pubbliche e commerciali,

quelle cui si accede mediante abbonamento o iscrizione a liste di distribuzione nonché la cd. “letteratura grigia”.

FONTE CHIUSA

- a) **Fonte documentale** da cui è possibile trarre notizie non pubblicamente disponibili.
- b) In gergo operativo, **fonte confidenziale** con cui sia cessato ogni rapporto di collaborazione.

FONTE CONFIDENZIALE

Soggetto, usualmente definito fiduciario, che fornisce in via confidenziale – e dunque con l’aspettativa che tanto l’apporto informativo quanto il rapporto con il servizio di informazione restino riservati – notizie di interesse per la sicurezza nazionale. Accanto ai rapporti di tipo strutturato, ne esistono altri di tipo estemporaneo: in tali ipotesi la fonte è definita “occasionale” e, se del caso, “non più contattabile”. Sono altresì frequentemente utilizzate le espressioni “fonte da cautelare”, per evidenziare la necessità di proteggere la fonte dall’eventuale **compromissione**, e “fonte in via di esperimento”, per sottolineare l’accentuata aleatorietà dell’apporto informativo. Nell’ordinamento italiano esistono specifiche disposizioni volte a tutelare la fonte confidenziale, consentendo che la sua identità venga sottaciuta anche a fronte di espressa richiesta dell’Autorità giudiziaria.

Vedi anche **GESTIONE DELLE FONTI**

FONTE DOCUMENTALE

Supporto analogico o digitale contenente notizie di interesse per la sicurezza nazionale.

Vedi anche **FONTE CHIUSA**

FONTI TECNICHE

Sistema tecnologico (per es. radar) che rileva/capta e registra notizie di interesse per la sicurezza nazionale.

FONTI UMANE

Vedi **FONTI CONFIDENZIALI**

FUNZIONARIO ALLA SICUREZZA

Nell'ambito delle amministrazioni pubbliche, degli enti pubblici e privati e degli operatori economici abilitati a trattare informazioni classificate, è il soggetto cui possono essere affidati, per delega del vertice dell'organizzazione, compiti di direzione, coordinamento, controllo, ispettivi e di inchiesta in materia di tutela della **sicurezza delle informazioni**. Per l'esercizio delle sue funzioni, il funzionario alla sicurezza – che nell'ambito dell'Amministrazione della Difesa assume la denominazione di "Ufficiale alla sicurezza" – si avvale del supporto di altre figure nei settori della trattazione e gestione dei documenti classificati, nonché della sicurezza fisica, informatica e delle comunicazioni.

G

GARANZIE FUNZIONALI

Speciali cause di giustificazione previste per gli appartenenti ai servizi di informazione che pongano in essere condotte configurabili come reato, a condizione di essere stati a ciò autorizzati ai fini dello svolgimento dei compiti istituzionali. Tale **strumento operativo** è disciplinato nel dettaglio dalla legge che ha previsto specifiche procedure (rimettendo al Presidente del Consiglio dei ministri o all'Autorità delegata, ove istituita, l'autorizzazione ovvero la ratifica delle condotte), condizioni (relative, tra l'altro, alla indispensabilità e proporzionalità della condotta) e limiti (per quanto riguarda, ad esempio, l'esclusione di una serie di figure di reato dall'ambito di applicabilità delle garanzie funzionali).

Si applicano anche a soggetti esterni che agiscano in concorso con dipendenti dell'Agenzia informazioni e sicurezza esterna o dell'Agenzia informazioni e sicurezza interna, laddove il ricorso alla loro opera sia indispensabile e sia stato autorizzato.

GEOINT (GEOSPATIAL INTELLIGENCE)

Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale provenienti da dati ed immagini georeferenziati.

GESTIONE DELLE FONTI

Complesso delle attività finalizzate ad individuare, valutare e reclutare una **fonte confidenziale** e, una volta

instaurato un rapporto di collaborazione, dirigerne, coordinarne e controllarne l'azione, anche nell'ottica di evitarne la **compromissione**. Tipica di tale ambito è l'espressione "coltivare una fonte", per indicare l'insieme delle iniziative intese a garantirsi la collaborazione di un soggetto e la sua lealtà. I tentativi di sistematizzare la materia hanno generato, Oltreoceano, il conio del termine MICE – acronimo degli inglesi denaro/ideologia/coercizione/egotismo – per indicare i motivi che più frequentemente inducono una persona a collaborare con i servizi di informazione.

Vedi anche **RICERCA INFORMATIVA**

GESTORE (CASE OFFICER)

Appartenente ad un servizio di informazione incaricato di gestire agenti, fonti confidenziali e/o operazioni.

GREY LITERATURE

Vedi **LETTERATURA GRIGIA**

GROUPTHINK

Una delle possibili "patologie" dell'attività di analisi: è il meccanismo in base al quale un gruppo, non di rado muovendo da preconcetti o stereotipi ed operando in un clima lavorativo che sopprime il dissenso, privilegia l'unanimità a scapito della qualità e non considera le alternative possibili, approdando così a conclusioni errate.

H

HUMINT (HUMAN INTELLIGENCE)

Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale provenienti da persone fisiche. Le sue specificità sono legate alla tipicità della fonte e si sostanziano soprattutto in particolari modalità di gestione.

Vedi anche **FONTE CONFIDENZIALE** e **GESTIONE DELLE FONTI**

HJK

I

IDENTITÀ DI COPERTURA

Identità sotto cui si cela, per evitare la **compromissione**, un **agente**, che si avvale a tale fine anche di una storia di copertura, ossia di un insieme di precedenti biografici e professionali diversi da quelli reali. Nell'ambito del Sistema di informazione per la sicurezza della Repubblica, l'uso di documenti e certificati di copertura da parte degli operatori dei servizi di informazione deve essere autorizzato dal Direttore generale del Dipartimento delle informazioni per la sicurezza, previa comunicazione al Presidente del Consiglio dei ministri o all'Autorità delegata, ove istituita. Tali documenti non conferiscono la qualità di agente/ufficiale di polizia giudiziaria, di pubblica sicurezza o di polizia tributaria.

IMINT (IMAGERY INTELLIGENCE)

Disciplina intelligence consistente nell'elaborazione di immagini di interesse per la sicurezza nazionale acquisite tramite sistemi fotografici, radar, elettro-ottici o sensori all'infrarosso o termici basati a terra, su unità navali o su vettori aero-spaziali.

INDICATORI CHIAVE

Dati o eventi che riflettono l'intento e/o la capacità di un attore ostile o comunque di interesse informativo di adottare una determinata linea d'azione ovvero la possibilità che un fenomeno o una situazione evolvano in una determinata direzione.

INDICATORI D'ALLARME

Dati o eventi relativi ad una minaccia concreta ed attuale alla sicurezza nazionale. Sulla base di tali indicatori sono prodotti e disseminati specifici allerta (cd. "*warning*").

INFILTRATO

Agente di cui si avvale un servizio di informazione per acquisire notizie in ambienti od organizzazioni di interesse.

Vedi anche **PENETRAZIONE INFORMATIVA**

INFLUENZA

Attività condotta da soggetti, statuali o non, al fine di orientare a proprio vantaggio le opinioni di un individuo o di un gruppo.

Vedi anche **INFORMATION WARFARE**

INFORMATION ASSURANCE (IA)

Insieme delle misure adottate per difendere le informazioni ed i sistemi informativi così da garantire la loro disponibilità, integrità, autenticazione, riservatezza e “non disconoscibilità” (consistente nella prova certificabile che un utente ha compiuto una determinata azione). Comprende la **COMPUSEC**, la **COMSEC**, l'**INFOSEC** e le misure **TEMPEST** ed include le attività finalizzate ad assicurare il ripristino dei sistemi informativi a seguito di attacchi o *failure*.

INFORMATION WARFARE

Concetto basato sull'idea che quello informativo sia un vero e proprio nuovo dominio in cui, tra stati ovvero tra stati ed attori non statuali, si gioca un confronto che vede le informazioni costituire, ad un tempo, strumento di offesa ed obiettivo. In questo contesto, il termine indica le azioni intraprese al fine di acquisire superiorità nel dominio informativo minando i sistemi, i processi ed il patrimonio informativo dell'avversario e difendendo al contempo i propri sistemi e le proprie reti nonché, più in generale, l'impiego delle informazioni ai fini del perseguimento degli interessi nazionali. Così concepita, include anche una serie di attività tipiche della tradizione intelligence – ma che oggi possono avvalersi delle potenzialità offerte dal progresso tecnologico – quali la **disinformazione**, l'**influenza** e la **controinformazione**, appartenenti alla categoria delle cd. “*psyops*”.

INFORMATIVA

Vedi **PRODOTTI INTELLIGENCE**

INFORMATORE

Vedi **FONTE CONFIDENZIALE**

INFORMAZIONE

- a) Il prodotto dell'**elaborazione** di una o più **notizie** di interesse per la sicurezza nazionale. In tal senso corrisponde all'analogia accezione del termine inglese "intelligence" (vedi anche **INFORMAZIONI INTELLIGENCE**).
- b) In tema di tutela della sicurezza delle informazioni, il termine ha valenza generica ricomprendendo atti, documenti, notizie, attività ed ogni altra cosa assistiti dal vincolo del **segreto di Stato** (cd. "informazione coperta da segreto di Stato") o cui sia stata attribuita una **classifica di segretezza** (cd. "informazione classificata").

INFORMAZIONE CLASSIFICATA

Vedi **INFORMAZIONE** sub b)

INFORMAZIONI INTELLIGENCE

Sebbene di uso corrente, l'espressione è in realtà tautologica in quanto il termine **informazioni** coincide con l'inglese "intelligence". Viene impiegata per sottolineare la tipicità del metodo di acquisizione e del processo di elaborazione cui sono sottoposte le notizie nonché la loro precipua finalità di tutela della sicurezza nazionale.

INFORMAZIONI NON CLASSIFICATE CONTROLLATE

Informazioni prive di classifica di segretezza, ma ritenute comunque meritevoli di protezione, ad esempio attraverso la limitazione dell'accesso alle sole persone che

hanno necessità di trattarle per motivi attinenti al loro impiego, incarico o professione.

INFORMAZIONI SENSIBILI

Informazioni, classificate o meno, la cui conoscenza da parte di attori ostili, statuali o non, può risultare pregiudizievole alla sicurezza nazionale.

INFOSEC (INFORMATION SECURITY)

Complesso delle misure di sicurezza volte a garantire **integrità**, riservatezza e disponibilità delle informazioni classificate o coperte da segreto di Stato e dei correlati sistemi informativi e di comunicazione, per esempio attraverso l'**autenticazione** degli utenti. Include le misure necessarie a rilevare e contrastare eventuali intrusioni. L'attuale dottrina in tema di sicurezza di reti e sistemi ha inglobato l'INFOSEC nell'**Information Assurance**.

INFRASTRUTTURE CRITICHE

Sistemi, risorse e reti, e loro insiemi – sia fisici che virtuali – essenziali per lo svolgimento delle funzioni vitali di uno o più Stati.

INGERENZA

Intromissione negli affari interni di un paese al fine di influenzarne le decisioni e le condotte a proprio vantaggio. La concezione tradizionale è legata all'idea del confronto tra stati e vede nell'ingerenza una delle minacce tipiche alla sovranità nazionale. Oggi, peraltro, il termine si rife-

risce frequentemente alle azioni poste in essere da attori non statuali e riguarda in modo crescente il campo economico-finanziario, dove l'acquisizione di posizioni dominanti in settori di interesse strategico risulta in grado di tradursi in un forte potere di condizionamento delle scelte di governo.

INTEGRAZIONE

Fase dell'**analisi** in cui un'**informazione** viene sistematizzata all'interno di un pregresso quadro conoscitivo ed arricchita di ulteriori elementi, già validati ed eventualmente tratti da altre fonti.

INTEGRITÀ

Condizione di un dato o di un'informazione che non siano stati incidentalmente o intenzionalmente modificati, alterati o distrutti e mantengano quindi il loro contenuto originario.

INTELLIGENCE

a) Il prodotto dell'**elaborazione** di una o più **notizie** di interesse per la sicurezza nazionale. In questa accezione, corrisponde al termine **informazione**, come utilizzato dal Legislatore italiano nella legge istitutiva del Sistema di informazione per la sicurezza della Repubblica.

Il vocabolo, largamente impiegato anche in ambito nazionale, ha valenza generica; viene quindi spesso ac-

compagnato da aggettivi intesi a specificarne finalità (strategica, tattica, operativa), natura (situazionale o previsionale), fonte di provenienza o materia cui si riferisce (economico-finanziaria, militare, etc.).

- b) Insieme delle funzioni, delle attività e degli organismi coinvolti nel processo di pianificazione, ricerca, elaborazione e disseminazione di informazioni di interesse per la sicurezza nazionale.

Vedi anche **CICLO INTELLIGENCE**

INTELLIGENCE AD IMMEDIATO IMPATTO OPERATIVO

Informazioni che consentono ai fruitori istituzionali (decisore politico, comandante militare, Forze di polizia, etc.) di assumere iniziative immediate per contrastare/contenere una **minaccia** imminente. Il concetto è impiegato soprattutto nel mondo anglosassone, con l'espressione *actionable intelligence*.

INTELLIGENCE "CIRCOLARE"

Una delle possibili "patologie" dell'attività di analisi: è il meccanismo per cui due soggetti si inducono reciprocamente in errore poiché traggono dalla condivisione di una medesima notizia non confermata o previsione errata il convincimento che essa sia attendibile in quanto riscontrata dall'altro.

INTELLIGENCE DI BASE

Informazioni su ambiti tematici, fenomeni, eventi, aree geografiche e soggetti/organizzazioni, impiegate quale materiale di riferimento per la **pianificazione informativa**

o l'**analisi** di informazioni di interesse per la sicurezza nazionale.

INTELLIGENCE ECONOMICO-FINANZIARIA

Ricerca ed elaborazione di notizie finalizzate alla tutela degli interessi economici, finanziari, industriali e scientifici di un paese ad opera dei suoi servizi di informazione. Si occupa tanto della **minaccia economico-finanziaria** quanto dei circuiti finanziari correlati ad altri fattori di minaccia, quali il terrorismo e la proliferazione di armi di distruzione di massa. Pure ricompresa da diversi paesi nella sfera dell'intelligence economico-finanziaria l'attività di ricerca ed elaborazione di notizie volta ad individuare nuove e/o migliori opportunità di crescita per il proprio sistema economico-finanziario.

INTELLIGENCE GREZZA

Termine colloquiale impiegato per indicare notizie non ancora sottoposte ad **elaborazione**.

INTELLIGENCE MILITARE

- a) Informazioni relative alla dottrina militare ed alle capacità belliche di un paese straniero.
- b) Informazioni a supporto dei contingenti militari nazionali nei teatri di crisi.

INTELLIGENCE OPERATIVA

Informazioni atte a supportare la pianificazione e la condotta delle operazioni dei servizi di informazione.

INTELLIGENCE STRATEGICA

Informazioni atte a supportare l'adozione di politiche interne ed internazionali in materia di sicurezza nazionale. Si caratterizza per la capacità di integrare elementi molteplici, funzionali a cogliere le tendenze di fenomeni e situazioni, individuando le vulnerabilità ed opportunità ad esse collegate.

INTELLIGENCE TATTICA

Informazioni atte a supportare i fruitori istituzionali nell'adozione di scelte contingenti.

INTELLIGENCE TECNICA

Informazioni relative alle capacità scientifiche e tecnologiche, specie in campo militare, di stati esteri.

INTERCETTAZIONI PREVENTIVE

Strumento disciplinato dalle norme di attuazione, di coordinamento e transitorie del codice di procedura penale di cui possono avvalersi anche i servizi di informazione – sulla base di delega da parte del Presidente del Consiglio dei ministri o dell'Autorità delegata, ove istituita, e di autorizzazione del Procuratore Generale presso la Corte di Appello di Roma – quando sia ritenuto indispensabile per l'espletamento delle attività loro demandate dalla legge.

INTERPRETAZIONE

Fase dell'**analisi** in cui si determina la pregnanza di un'informazione, ossia quanto questa confermi o innovi il patrimonio informativo.

INTERVISTA

In gergo operativo, indica l'interlocuzione di un appartenente ad un servizio di informazione con una **fonte confidenziale**, inclusa quella di natura estemporanea ignara delle finalità dell'intervistatore.

INTOSSICAZIONE

Particolare tipologia di **disinformazione**, consistente nel far giungere ad uno stato ostile e/o ai suoi servizi di informazione notizie false per inficiarne funzione informativa e processi conoscitivi e decisionali.

Vedi anche **DISINFORMAZIONE** e **PSYOPS**

L

LETTERATURA GRIGIA

Concetto elaborato, con il nome di “*grey literature*”, nell’ambito della dottrina anglosassone sulle fonti aperte. Identifica notizie o dati pubblicamente disponibili, ma ad accesso limitato e dunque più difficili da individuare. Include atti di convegni e conferenze, rapporti, documenti e studi governativi ed accademici – anche non ufficiali – documenti/ricerche aziendali e di mercato.

LISTA DI ACCESSO

Elenco dei soggetti autorizzati dal **funzionario alla sicurezza**, sulla base della **necessità di conoscere**, a trattare informazioni classificate SEGRETO e SEGRETISSIMO nonché quelle cui sia stata attribuita una **qualifica di sicurezza**.

LIVELLI DI SEGRETEZZA

Vedi **CLASSIFICA DI SEGRETEZZA**

LUOGHI DI INTERESSE PER LA SICUREZZA DELLA REPUBBLICA

Strutture, o parti di esse, essenziali a garantire la continuità dell’azione di governo, la funzionalità dei sistemi di telecomunicazione e di allerta rilevanti ai fini della gestione delle crisi ed il funzionamento dell’apparato economico, produttivo e logistico nazionale, nonché l’attività di qualunque altra infrastruttura critica, pubblica o

privata, soggetta alla sovranità nazionale. Sono altresì luoghi di interesse per la sicurezza della Repubblica le strutture delle amministrazioni che esercitano competenze istituzionali in materia di difesa e sicurezza dello Stato e di polizia. A tali luoghi si applicano regole di accesso e controllo intese ad assicurare adeguati profili di tutela.

M

MASINT

(MEASUREMENT AND SIGNATURE INTELLIGENCE)

Disciplina intelligence consistente nella ricerca ed elaborazione di elementi tecnico-scientifici relativi ad attributi fisici (dati metrici, angolari, spaziali, di lunghezza d'onda, etc.) di eventi ed obiettivi di interesse informativo al fine di localizzarli ed individuarne le caratteristiche salienti. Consente, per esempio, di rilevare esplosioni nucleari connesse alla sperimentazione di armi di distruzione di massa.

MATERIALE CRITTOGRAFICO

Vedi **MATERIALI E DOCUMENTAZIONE COMSEC**

MATERIALI DUAL USE

Macchinari, componentistica, etc. che, sebbene non progettati o sviluppati per uso militare, possono tuttavia essere impiegati, preve eventuali modifiche, per lo sviluppo, la produzione o l'utilizzo di armi e sistemi d'arma. Vedi anche **CONTROPROLIFERAZIONE**

MATERIALI E DOCUMENTAZIONE COMSEC

Algoritmi e logiche crittografiche, apparecchiature e sistemi, chiavi di cifratura e relative pubblicazioni impiegati per garantire la sicurezza della trasmissione delle informazioni classificate.

Vedi anche **COMSEC**

MEDINT (MEDICAL INTELLIGENCE)

Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale di natura bio-scientifica, bio-medica, epidemiologica, ambientale ed altro, relative alla salute umana o veterinaria.

MINACCIA

Fenomeno, situazione e/o condotta potenzialmente lesivi della **sicurezza nazionale**. Può essere rappresentata dalle attività di stati, di organizzazioni non statuali o di singoli individui. A seconda delle forme di estrinsecazione, degli agenti, del bene aggredito e del contesto viene definita come minaccia criminale, minaccia terroristica, minaccia economica, minaccia transnazionale, etc.

MINACCIA ASIMMETRICA

Concetto originariamente sviluppato in ambito militare, indica l'uso – al fine di colmare lo svantaggio nei confronti dell'avversario – di metodi di aggressione diversi da quelli tradizionali, spesso in danno di obiettivi civili, intesi a produrre anche un serio impatto psicologico. Tipicamente asimmetrica è la minaccia terroristica.

MINACCIA CBRN

Possibile uso, da parte di un soggetto ostile, di agenti **Chimici**, **Biologici**, **Radiologici** o **Nucleari** o delle relative armi. Al fine di adeguarlo alle più diffuse tendenze operative del terrorismo, specie nei teatri di crisi, l'acronimo CBRN si è negli ultimi anni arricchito di una "E" finale, per includervi la minaccia collegata all'uso di **Esplosivi**

(eventualmente associati agli agenti citati nelle cd. “*dirty bomb*”, bombe sporche).

Vedi anche **MINACCIA NON CONVENZIONALE**

MINACCIA CIBERNETICA

Espressione impiegata per indicare l’insieme delle condotte controindicate che possono essere realizzate nel e tramite il *cyber-space* ovvero in danno di quest’ultimo e dei suoi elementi costitutivi. Si sostanzia in attacchi cibernetici: azioni di singoli individui o organizzazioni, statuali e non, finalizzate a distruggere, danneggiare o ostacolare il regolare funzionamento dei sistemi e delle reti e/o dei sistemi attuatori di processo da essi controllati, ovvero a violare integrità e riservatezza di dati/informazioni.

A seconda degli attori e delle finalità, si parla di:

- criminalità cibernetica (*cyber-crime*): complesso delle attività con finalità criminali (quali, per esempio, la truffa o frode telematica, il furto d’identità, la sottrazione indebita di informazioni o di creazioni e proprietà intellettuali);
- spionaggio cibernetico (*cyber-espionage*): acquisizione indebita di dati/informazioni sensibili, proprietarie o classificate;
- terrorismo cibernetico (*cyber-terrorism*): insieme delle azioni ideologicamente motivate, volte a condizionare uno stato o un’organizzazione internazionale.

Tale categorizzazione ha valenza meramente descrittiva, fermo restando che, in concreto, l’azione controindicata spesso non presenta alcuna caratterizzazione peculiare: un’intrusione in un sistema informatico, per esempio, può essere strumentale tanto alla sottrazione di dati per

fini di lucro (matrice criminale) quanto ad intenti spionistici o terroristici oppure, ancora, ad attività di cd. *“hacktivism”* o *“cyber agitation”* (l’impiego di computer e di sistemi correlati, con o senza il ricorso a tecniche di hackeraggio, quale forma di protesta ideologicamente motivata).

MINACCIA CONVENZIONALE

Possibile impiego del dispositivo bellico da parte di un paese ostile secondo precise regole di dottrina e tattica militari.

MINACCIA CRIMINALE

Minaccia costituita dalla **criminalità organizzata**.

MINACCIA ECONOMICO-FINANZIARIA

Insieme dei fenomeni di illegalità economica (riciclaggio, pratiche distorsive del mercato, evasione fiscale e contributiva, contraffazione e contrabbando, etc.) e delle attività in danno degli interessi economici, finanziari, industriali e scientifici poste in essere da soggetti, statuali o non, con particolare riguardo a: infrastrutture critiche; livelli occupazionali e produttivi; patrimonio tecnologico e scientifico; libera concorrenza e operatività dei mercati finanziari.

MINACCIA EVERSIVA

Minaccia costituita dall’**eversione**.

MINACCIA NON CONVENZIONALE

Possibile uso, da parte di un soggetto ostile, statuale o non, di metodologie di attacco diverse da quelle tradizionali. In un'accezione tecnica indica la cd. "minaccia CBRN". Vedi anche **MINACCIA ASIMMETRICA**

MINACCIA TERRORISTICA

Minaccia costituita dal **terrorismo**.

MINACCIA TRANSNAZIONALE

Espressione generica utilizzata per indicare fenomeni, situazioni e/o condotte potenzialmente lesivi della sicurezza nazionale che interessano più ambiti territoriali e sono non di rado riconducibili ad attori di varia nazionalità. Hanno da tempo caratura transnazionale le principali minacce alla sicurezza, dal terrorismo alla criminalità organizzata, dalla minaccia economico-finanziaria a quella cibernetica. Del resto, pure minacce tradizionalmente "interne", come l'anarco-insurrezionalismo e la criminalità organizzata "autoctona", presentano attualmente una dimensione "esterna", per quanto riguarda sfere di operatività ed ambiti di riferimento e/o ispirazione. Per indicare la pervasività ed il potenziale impatto sulla stabilità internazionale di taluni fenomeni si ricorre frequentemente al concetto di "minaccia globale".

MISSIONE

Insieme dei compiti affidati agli organismi informativi. In ambito operativo, è lo scopo specifico da perseguire attraverso la **ricerca informativa**.

MODELLO OPERATIVO

Insieme di concetti e regole impiegati per strutturare la **ricerca informativa** secondo principi di efficacia ed efficienza. Prevede la definizione delle minacce e dei correlati processi di acquisizione delle notizie di interesse e l'individuazione di idonee risorse e tattiche al fine di prevenire, rilevare, contenere e contrastare le minacce alla sicurezza nazionale.

MONITORAGGIO INFORMATIVO

Attività di **ricerca informativa** svolta con carattere di continuità in direzione di un obiettivo (vedi **OBIETTIVO DI RICERCA**) al fine di cogliere gli **indicatori chiave** o **d'allarme**.

N

NECESSITÀ DI CONOSCERE

Principio che subordina l'**accesso** a determinate informazioni all'effettiva indispensabilità ai fini dello svolgimento di specifici compiti istituzionali.

In materia di tutela della sicurezza delle informazioni, è una condizione aggiuntiva rispetto al possesso del **Nulla Osta di Sicurezza** per accedere ad informazioni con classifica superiore a RISERVATO.

Vedi anche **COMPARTIMENTAZIONE**

NEED TO KNOW

Vedi **NECESSITÀ DI CONOSCERE**

NOS

Vedi **NULLA OSTA DI SICUREZZA**

NOTIZIE

Elementi conoscitivi di interesse ai fini della sicurezza nazionale acquisiti mediante **ricerca informativa**.

NULLA OSTA DI SICUREZZA (NOS)

Abilitazione di sicurezza che consente alle persone fisiche di trattare informazioni con **classifica di segretezza** superiore a RISERVATO. Non può essere richiesta dal singolo, ma solo da soggetti pubblici o da operatori economici

abilitati a trattare informazioni classificate. Al rilascio del NOS ed eventualmente alla sua revoca, sospensione o limitazione provvedono – sulla base di un accertamento dell'**affidabilità** dell'interessato – l'Ufficio centrale per la segretezza ovvero le articolazioni dell'**Organizzazione nazionale per la sicurezza** dallo stesso delegate.

Ha validità decennale per le classifiche di segretezza RISERVATISSIMO e SEGRETO, quinquennale per il SEGRETISSIMO.

NULLA OSTA DI SICUREZZA INDUSTRIALE (NOSI)

Abilitazione di sicurezza che consente agli operatori economici di trattare informazioni classificate e partecipare a gare d'appalto per l'affidamento di contratti classificati SEGRETO o SEGRETISSIMO ovvero qualificati NATO o UE e di eseguire lavori, fornire beni e servizi, realizzare opere, studi e progettazioni ai quali sia attribuita una **classifica di segretezza** superiore a RISERVATO. L'Ufficio centrale per la segretezza provvede al rilascio – ed eventualmente alla revoca, sospensione o limitazione – del NOSI sulla base di un accertamento dell'**affidabilità** dell'operatore economico. Ha validità decennale fino a livello SEGRETO, quinquennale se a livello SEGRETISSIMO.

Vedi anche **ABILITAZIONE PREVENTIVA**

O

OBIETTIVI INFORMATIVI

Ambiti tematici, fenomeni, eventi, aree geografiche e soggetti/organizzazioni che costituiscono esplicitazione del **fabbisogno informativo** delle Autorità di governo in materia di sicurezza nazionale. Fissano – secondo una scala di priorità – la **missione** del comparto informativo, dando avvio al **ciclo intelligence**. In Italia, sono definiti annualmente dal Comitato interministeriale per la sicurezza della Repubblica. Vedi anche **PIANIFICAZIONE INFORMATIVA**

OBIETTIVO DI RICERCA

Ambito tematico, fenomeno, evento, area geografica e soggetto/organizzazione su cui deve concentrarsi la **ricerca informativa**. È di norma specificato nel **piano di ricerca**, salvo che non emerga da esigenze informative contingenti.

OMOLOGAZIONE

Provvedimento con cui l'Ufficio centrale per la segretezza certifica l'idoneità di sistemi, apparati, dispositivi ed impianti a trattare informazioni classificate. È previsto per i sistemi informativi, TEMPEST e di comunicazione e trasmissione dati – assumendo rispettivamente il nome di OMOLOGAZIONE EAD (elaborazione automatica dei dati), OMOLOGAZIONE TEMPEST ed OMOLOGAZIONE COMSEC – ed è il frutto di una valutazione che tiene tra l'altro conto dell'analisi del rischio e della rispondenza a specifici requisiti tecnici e di sicurezza.

OPERAZIONE

Attività info-operativa, circoscritta nel tempo e nello spazio, volta al perseguimento di una specifica missione.

OPERAZIONE SOTTO COPERTURA

Attività info-operativa condotta in modo da celare/dissimulare l'identità degli **agenti** e la riconducibilità delle strutture impiegate ad un servizio di informazione.

Vedi anche **IDENTITÀ DI COPERTURA** ed **ATTIVITÀ ECONOMICHE SIMULATE**

OPPOSIZIONE DEL SEGRETO DI STATO

Atto con cui viene eccepita all'Autorità giudiziaria l'esistenza del **segreto di Stato**. L'opposizione deve essere confermata dal Presidente del Consiglio dei ministri entro 30 giorni con atto motivato, avverso il quale può essere sollevato conflitto di attribuzione dinanzi alla Corte Costituzionale.

Un caso particolare concerne l'acquisizione mediante intercettazione, da parte dell'Autorità giudiziaria, di comunicazioni di servizio di appartenenti agli organismi informativi: in tale ipotesi, l'eventuale opposizione del segreto di Stato deve intervenire ad opera del Presidente del Consiglio dei ministri entro 60 giorni dalla notificazione della richiesta dell'Autorità giudiziaria intesa a conoscere se talune delle informazioni così acquisite, di cui la stessa intenda avvalersi nel processo, siano coperte da segreto.

ORGANISMO INFORMATIVO

Organizzazione appartenente alla **comunità intelligence**.

ORGANIZZAZIONE NAZIONALE PER LA SICUREZZA

Il complesso degli organi e delle articolazioni pubbliche e private legittimate a trattare informazioni classificate o coperte da segreto di Stato, di cui si avvale l'**Autorità nazionale per la sicurezza** al fine di assicurare modalità di gestione e trattazione uniformi e sicure, nonché la protezione ininterrotta delle informazioni. Si articola in: Organo nazionale di sicurezza (funzione svolta dal Direttore generale del **Dipartimento delle informazioni per la sicurezza**); Ufficio centrale per la segretezza; organi di sicurezza operanti a livello centrale e periferico presso pubbliche amministrazioni, enti pubblici e privati ed operatori economici abilitati.

OSINT (OPEN SOURCE INTELLIGENCE)

Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale tratte da **fonti aperte**.

L'eccezionale crescita delle notizie pubblicamente disponibili registrata negli ultimi anni ha conferito all'OSINT una significativa rilevanza anche nell'ambito delle attività di informazione per la sicurezza ai fini dell'analisi integrata di fenomeni e situazioni di interesse (vedi **ALL-SOURCE INTELLIGENCE**), consentendo altresì di focalizzare le altre discipline intelligence sulle fonti "coperte". L'attività OSINT viene strutturata in fasi che ricalcano il **ciclo intelligence**: la peculiarità delle fonti impiegate e la vastità del loro numero richiedono, peraltro, peculiare attenzione tanto nell'individuazione preventiva e nella selezione delle fonti rilevanti, quanto nella determinazione del loro grado di attendibilità.

P

PATRIMONIO INFORMATIVO

Complesso di notizie e informazioni su ambiti tematici, fenomeni, eventi, aree geografiche e soggetti/organizzazioni di interesse per la sicurezza nazionale detenuto da un organismo informativo per l'adempimento dei compiti istituzionali.

PENETRAZIONE INFORMATIVA

Attività info-operativa condotta da un servizio di informazione per acquisire notizie in ambienti o organizzazioni di interesse, avvalendosi di uno o più infiltrati.

PIANIFICAZIONE INFORMATIVA

Fase del **ciclo intelligence** in cui vengono individuate le attività e le risorse necessarie per il perseguimento degli **obiettivi informativi**. L'esito è trasfuso nel **piano di ricerca**.

PIANO DI RICERCA

Documento con cui viene impostata la **ricerca informativa**, mediante la trasposizione degli **obiettivi informativi** in concreti, specifici **obiettivi di ricerca**, assegnati alle competenti articolazioni con le risorse necessarie.

PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Vertice del Sistema di informazione per la sicurezza della Repubblica, cui sono attribuite in via esclusiva:

- l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza, nell'interesse e per la difesa della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento;
- l'apposizione e la conferma dell'opposizione del **segreto di Stato**, nonché, in qualità di **Autorità nazionale per la sicurezza**, la sua tutela;
- la nomina e la revoca dei vertici e dei vice direttori del Dipartimento delle informazioni per la sicurezza, dell'Agazia informazioni e sicurezza esterna e dell'Agazia informazioni e sicurezza interna;
- la determinazione dell'ammontare annuo delle risorse finanziarie per gli organismi informativi.

Può delegare ad un Ministro senza portafoglio o ad un Sottosegretario di Stato, che assumono la denominazione di Autorità delegata, le funzioni che non gli sono attribuite in via esclusiva.

Presiede il Comitato interministeriale per la sicurezza della Repubblica.

PROCESSO INFORMATIVO

La successione delle attività concettuali, organizzative, operative ed esecutive attraverso le quali vengono acquisite ed elaborate le notizie di interesse per la sicurezza nazionale necessarie a soddisfare il **fabbisogno informativo** secondo i passaggi schematizzati nel **ciclo intelligence**.

PRODOTTI INTELLIGENCE

Comunicazioni in forma scritta od orale in cui viene trasferito il risultato della ricerca ed elaborazione di notizie di interesse per la sicurezza nazionale. Prende il nome di “informativa” il documento contenente informazioni di immediato interesse (l’esempio tipico è l’informativa concernente una minaccia di attentato terroristico), mentre assumono varia veste (punti di situazione, monografie, etc.) i prodotti in cui confluiscono le valutazioni degli analisti.

PRODUZIONE

Fase dell’**elaborazione** consistente nella redazione di **prodotti intelligence** per la successiva disseminazione ai fruitori istituzionali.

PSYOPS (PSYCHOLOGICAL OPERATIONS)

“Operazioni psicologiche” consistenti nel far giungere a comunità, organizzazioni e soggetti stranieri informazioni selezionate al fine di orientarne a proprio vantaggio opinioni e comportamenti.

Vedi anche **INFORMATION WARFARE**

Q

QUALIFICA DI SICUREZZA

Sigla (es. NATO e UE) o altro termine convenzionale (es. COSMIC) che, attribuiti ad un'informazione, classificata o meno, indicano l'organizzazione internazionale/comunitaria o il programma intergovernativo entro cui tale informazione è stata originata (ad opera di un'articolazione dell'organizzazione internazionale ovvero di un suo stato membro) e nel cui ambito può circolare. Nel contesto dell'Alleanza atlantica, le qualifiche in uso sono: COSMIC (per TOP SECRET, equivalente al SEGRETISSIMO italiano) e NATO (da SEGRETO a NON CLASSIFICATO).

Vedi anche **DEQUALIFICA**

R

RACCOLTA INFORMATIVA

Vedi RICERCA INFORMATIVA

REGOLA DELLA TERZA PARTE

Principio su cui si basano i rapporti di scambio informativo nell'ambito della **collaborazione internazionale intelligence**. Prevede che le notizie/informazioni acquisite da un **servizio collegato** non possano essere diffuse dal destinatario ad un altro organismo informativo estero senza il consenso dell'originatore. Tale regola opera tacitamente ed in via di prassi – e quindi a prescindere dalla circostanza che essa sia codificata o venga espressamente menzionata – e vale a tutelare in primo luogo la confidenzialità dello scambio informativo, evitando che notizie sensibili giungano a destinatari “indesiderati”. Ulteriore finalità risiede nello scongiurare “false” conferme dell'attendibilità di una notizia/informazione conseguenti a “rimbalzo” informativo e non ad autonome acquisizioni di altro servizio di informazione.

RELAZIONE AL PARLAMENTO

Documento pubblico annuale con il quale il Governo, entro il mese di febbraio, riferisce al Parlamento sulla politica dell'informazione per la sicurezza e sui risultati ottenuti l'anno precedente. Contiene un allegato concernente le attività di protezione cibernetica e di tutela delle infrastrutture critiche materiali ed immateriali. In gergo viene definita “relazione annuale”.

RELAZIONE SULL'ATTIVITÀ DEI SERVIZI DI INFORMAZIONE

Documento classificato con il quale, entro i mesi di marzo e settembre, il Presidente del Consiglio dei ministri – per consentire l'esercizio delle funzioni di controllo – riferisce al Comitato parlamentare per la sicurezza della Repubblica sull'operato dei servizi di informazione, sulla gestione finanziaria e del personale degli organismi informativi, nonché in merito alla situazione ed ai pericoli per la sicurezza. In gergo viene definita "relazione semestrale".

RICERCA INFORMATIVA

Fase del **ciclo intelligence** consistente nell'impiego delle diverse fonti e nello svolgimento di **attività info-operativa** per acquisire notizie utili a prevenire, rilevare, contenere e contrastare le minacce alla sicurezza nazionale. Rientra in questa fase anche l'individuazione di nuove fonti per ottimizzare la copertura informativa degli obiettivi ricevuti.

Vedi anche **GESTIONE DELLE FONTI**

RIDUZIONE DELLA CLASSIFICA DI SEGRETEZZA

Vedi **DECLASSIFICA**

RISCHIO

Sebbene spesso impiegato come sinonimo di pericolo e minaccia, il termine indica un danno potenziale per la sicurezza nazionale che deriva da un evento (tanto intenzionale che accidentale) riconducibile ad una **minaccia** e dal-

la sua interazione con le vulnerabilità del sistema-Paese o di suoi settori ed articolazioni. Minacce, vulnerabilità ed impatto costituiscono, quindi, le variabili principali in funzione delle quali viene valutata l'esistenza di un rischio ed il relativo livello ai fini della sua gestione, ossia dell'adozione delle necessarie contromisure (tanto preventive che reattive).

RISERVATEZZA (OBBLIGO DI)

Il dovere di mantenere il segreto su ciò di cui si sia venuti a conoscenza in ragione dell'attività prestata che grava sul personale, in servizio ed in quiescenza, del Dipartimento delle informazioni per la sicurezza, dell'Agenzia informazioni e sicurezza esterna e dell'Agenzia informazioni e sicurezza interna, nonché sui soggetti che a qualsiasi titolo prestino o abbiano prestato la propria opera a favore degli organismi informativi.

RISERVATISSIMO (RR)

Vedi **CLASSIFICA DI SEGRETEZZA**

RISERVATO (R)

Vedi **CLASSIFICA DI SEGRETEZZA**

S

SCAMBIO INFORMATIVO

Condivisione su base bilaterale o multilaterale di notizie ed informazioni tra Forze di polizia ed organismi informativi ovvero tra questi ultimi ed i servizi collegati.

SCUOLA DI FORMAZIONE DEL SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA

Articolazione del Dipartimento delle informazioni per la sicurezza cui è affidato il compito di assicurare l'addestramento, la formazione di base e continuativa e l'aggiornamento del personale degli organismi informativi.

SEGRETERIA PRINCIPALE DI SICUREZZA

Articolazione organizzativa istituita presso pubbliche amministrazioni, enti pubblici e privati ed operatori economici abilitati, di cui si avvale il **funzionario alla sicurezza** per la gestione dei documenti classificati.

SEGRETEZZA (LIVELLI DI)

Vedi **CLASSIFICHE DI SEGRETEZZA**

SEGRETISSIMO (SS)

Vedi **CLASSIFICA DI SEGRETEZZA**

SEGRETO (S)

Vedi CLASSIFICA DI SEGRETEZZA

SEGRETO DI STATO

Vincolo posto dal Presidente del Consiglio dei ministri – mediante **apposizione, opposizione** ovvero conferma dell'opposizione – su atti, documenti, notizie, attività, cose e luoghi la cui conoscenza non autorizzata può danneggiare gravemente gli interessi supremi dello Stato.

La costruzione dell'istituto – concepito quale elemento di tenuta dell'intero sistema democratico – è volta da un lato, attraverso la previsione di limiti e garanzie, a circoscrivere e regolare l'utilizzo del segreto di Stato, dall'altro ad assicurarne l'effettività, limitando la conoscibilità delle notizie assistite da tale vincolo ad un novero estremamente ristretto di soggetti. In tale quadro il legislatore ha disciplinato anche il rapporto tra segreto di Stato e processo penale, stabilendo che l'esistenza del segreto di Stato impedisce all'Autorità giudiziaria l'acquisizione e l'utilizzazione, anche indiretta, delle notizie assistite dal vincolo, ferma restando la possibilità per il giudice di ricorrere ad altri strumenti di prova, purché gli stessi non incidano sul medesimo oggetto. Quanto a limiti e garanzie, la legge 124/2007:

- esclude tassativamente che il segreto di Stato possa riguardare informazioni relative a fatti eversivi dell'ordine costituzionale o concernenti fatti di terrorismo, delitti di strage, associazione a delinquere di stampo mafioso, scambio elettorale di tipo politico-mafioso;
- limita la durata del vincolo a 15 anni, ulteriormente prorogabili dal Presidente del Consiglio dei ministri per un periodo che non può complessivamente superare i 30 anni;

- impone al Presidente del Consiglio dei ministri di comunicare i casi di conferma dell'opposizione del segreto di Stato al Comitato parlamentare per la sicurezza della Repubblica, indicandone le ragioni essenziali. Su richiesta del Presidente del COPASIR, il Presidente del Consiglio dei ministri è tenuto ad esporre, in una seduta segreta, il quadro informativo idoneo a consentire l'esame nel merito della conferma dell'opposizione del segreto di Stato. Se ritiene infondata l'opposizione, il Comitato ne riferisce a ciascuna delle Camere per le conseguenti valutazioni;
- fa obbligo al Presidente del Consiglio dei ministri di motivare l'opposizione e la conferma dell'opposizione del segreto di Stato. Avverso tali atti può essere sollevato conflitto di attribuzione dinanzi alla Corte costituzionale, cui il segreto non può in alcun caso essere opposto.

SERVIZI

Termine colloquiale impiegato quale sinonimo di agenzie intelligence.

SERVIZIO COLLEGATO

Organismo informativo estero con cui la comunità intelligence nazionale o una sua componente mantiene rapporti di collaborazione/cooperazione formalmente autorizzati.

Vedi anche **ACCORDO DI COOPERAZIONE/COLLABORAZIONE e COLLABORAZIONE INTERNAZIONALE INTELLIGENCE**

SERVIZIO DI INFORMAZIONE

Organizzazione governativa cui è affidato il compito di ricercare, elaborare e disseminare, nei modi e nelle forme

previste dalla legge, informazioni utili a prevenire, rilevare, contenere e contrastare le minacce alla **sicurezza nazionale**. In Italia la locuzione è impiegata per indicare specificamente l'**Agenzia informazioni e sicurezza esterna** e l'**Agenzia informazioni e sicurezza interna**.

SICUREZZA CIBERNETICA

Vedi **CYBER-SECURITY**

SICUREZZA CRITTOGRAFICA

Vedi **COMSEC**

SICUREZZA DELLE COMUNICAZIONI

Vedi **COMSEC**

SICUREZZA DELLE INFORMAZIONI

Condizione in cui risulti garantita la non **compromissione** delle informazioni classificate o coperte da segreto di Stato, attraverso l'adozione di apposite norme e procedure in materia di abilitazioni di sicurezza, sicurezza fisica, informatica e delle comunicazioni.

SICUREZZA FISICA

Condizione in cui risulti garantita l'inviolabilità fisica di strutture, beni strumentali – compresi i sistemi informativi e di comunicazione – e di qualunque altro luogo dove sono trattate o custodite informazioni classificate o coperte da segreto di Stato, rispetto a condotte ed eventi lesivi, specie

di natura intrusiva. Viene perseguita attraverso l'adozione di specifiche procedure e misure di difesa attiva e passiva.

SICUREZZA INFORMATICA

Vedi INFOSEC e INFORMATION ASSURANCE

SICUREZZA NAZIONALE

Condizione in cui ad un paese risultino garantite piene possibilità di sviluppo pacifico attraverso la salvaguardia dell'intangibilità delle sue componenti costitutive, dei suoi valori e della sua capacità di perseguire i propri interessi fondamentali a cospetto di fenomeni, condotte ed eventi lesivi o potenzialmente tali. È un bene costituzionale che gode di tutela prioritaria.

A tale dimensione "oggettiva" del concetto di sicurezza nazionale ne viene spesso affiancata una "soggettiva", che indica la percezione, da parte dei cittadini, della capacità dello Stato di tutelare se stesso, la propria popolazione ed i propri interessi impiegando gli strumenti del potere nazionale (politici, economici, diplomatici, militari, informativi, etc.). Comunque si intenda definirla, la nozione di sicurezza nazionale – e quella, connessa, di interesse nazionale – mantiene in ogni caso una forte caratterizzazione dinamica, risultando legata tanto al grado di maturità del paese cui si riferisce quanto al contesto storico: ne costituisce esempio la rilevanza strategica assunta dai concetti di sicurezza economico-finanziaria e di sicurezza ambientale. Un'elencazione meramente indicativa degli elementi che rientrano nell'ambito della sicurezza nazionale – e sono come tali, oggetto di tutela ad opera del Sistema di informazione per la sicurezza della Repubblica – deve

senz'altro includere l'indipendenza, l'integrità e la sovranità della Repubblica, la comunità di cui essa è espressione, le istituzioni democratiche poste dalla Costituzione a suo fondamento, la personalità internazionale dello Stato, le libertà fondamentali ed i diritti dei cittadini costituzionalmente garantiti nonché gli interessi politici, militari, economici, scientifici ed industriali dell'Italia.

SIGINT (SIGNALS INTELLIGENCE)

Disciplina intelligence consistente nella ricerca ed elaborazione di notizie di interesse per la sicurezza originate da segnali e/o emissioni elettromagnetiche provenienti dall'estero. Le principali branche della SIGINT sono la **COMINT** e la **ELINT**.

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA

Il complesso degli organi cui è affidata, in Italia, secondo le rispettive competenze, l'**attività di informazione per la sicurezza** e la correlata azione di indirizzo politico. Istituito dalla legge 124/2007, è composto dal Presidente del Consiglio dei ministri – che ne costituisce il vertice – dal Comitato interministeriale per la sicurezza della Repubblica, dall'Autorità delegata ove istituita, dal Dipartimento delle informazioni per la sicurezza, dall'Agenzia informazioni e sicurezza esterna e dall'Agenzia informazioni e sicurezza interna.

SPIONAGGIO

Attività condotte da agenzie intelligence straniere nonché da individui od organizzazioni operanti in modo auto-

no o ovvero in collegamento con servizi di informazione esteri al fine di acquisire notizie in danno della sicurezza nazionale.

STEGANOGRAFIA

Processi e metodi per occultare un messaggio all'interno di un vettore (documentale o digitale). Usata sin dall'antichità (l'inchiostro cd. "simpatico" ne costituisce l'esempio tipico), ha conosciuto nuovi sviluppi con l'avvento della tecnologia dell'informazione, che consente di celare un messaggio all'interno di immagini o di *file* audio e video. Può associarsi al ricorso alla **crittografia**, da cui si differenzia poiché interviene non sul testo del messaggio trasmesso, ma sulla rilevabilità della stessa esistenza del messaggio. La disciplina che si occupa di individuare il ricorso alla steganografia è denominata steganalisi e presenta difficoltà aggiuntive rispetto alla **crittanalisi** poiché si cimenta con flussi di informazione che non è accertato contengano messaggi nascosti.

Vedi anche **CRITTOLOGIA**

STRUMENTI OPERATIVI

Mezzi e procedure di cui si possono avvalere i servizi di informazione per l'**attività info-operativa**. In Italia, tra essi figurano le **intercettazioni preventive**, le **attività economiche simulate**, le **garanzie funzionali** e le **identità di copertura**.

T

TEMPEST

Acronimo dell'espressione inglese "*Transient Electro Magnetic Pulse Emanation Standard*", indica le tecnologie atte ad eliminare o ridurre le emissioni prodotte dalle apparecchiature elettroniche che elaborano e trasmettono informazioni classificate o coperte da segreto di Stato per evitare che esse vengano captate da soggetti ostili.

TERRORISMO

Fenomeno consistente nell'uso ideologicamente motivato di violenza indiscriminata, ad opera di soggetti non statuali o singoli (con o senza l'appoggio di Stati cd. "sponsor") operanti in clandestinità (caratteristica, questa, che vale a distinguere il terrorismo da altre forme di conflittualità violenta), contro la popolazione civile, le istituzioni o gli interessi di uno stato ovvero in danno di un'organizzazione internazionale allo scopo di diffondere terrore e condizionarne orientamenti e scelte. Include anche le attività di tipo strumentale ed accessorio, comprese quelle di stampo propagandistico. Può essere ispirato da ideologie di tipo "laico" (tanto di estrema destra che di estrema sinistra), da rivendicazioni di carattere etnico o etnico-separatista ovvero da istanze confessionali.

U

UCSE

Vedi **UFFICIO CENTRALE PER LA SEGRETEZZA**

UFFICIALE ALLA SICUREZZA

Vedi **FUNZIONARIO ALLA SICUREZZA**

UFFICIO CENTRALE DEGLI ARCHIVI

Articolazione del Dipartimento delle informazioni per la sicurezza cui è affidato il compito di garantire uniformità di norme e procedure in materia archivistica nell'ambito degli organismi informativi. In tale contesto l'Ufficio, tra l'altro: coordina le attività di gestione degli archivi correnti del Dipartimento delle informazioni per la sicurezza, dell'Agencia informazioni e sicurezza esterna e dell'Agencia informazioni e sicurezza interna; vigila sulla loro corretta tenuta; gestisce l'archivio storico degli organismi informativi, cui compete versare all'Archivio centrale dello Stato la documentazione divenuta di libera consultazione.

UFFICIO CENTRALE ISPETTIVO

Articolazione del Dipartimento delle informazioni per la sicurezza cui è affidato il compito di verificare in via continuativa – attraverso ispettori ai quali è garantita piena autonomia ed indipendenza di giudizio anche grazie ad un peculiare regime giuridico loro riservato – che le attività condotte dall'Agencia informazioni e sicurezza esterna e dall'Agencia informazioni e sicurezza interna siano conformi a legge, regolamenti e direttive. Su autorizzazione

del Presidente del Consiglio dei ministri o dell’Autorità delegata, ove istituita, gli ispettori possono svolgere anche inchieste interne su specifici episodi e comportamenti verificatisi nell’ambito dei servizi di informazione.

UFFICIO CENTRALE PER LA SEGRETEZZA (UCSE)

Articolazione del Dipartimento delle informazioni per la sicurezza cui sono affidate funzioni direttive, consultive, di coordinamento e controllo in materia di tutela amministrativa del **segreto di Stato** e delle **classifiche di segretezza**. In tale ambito l’UCSE, tra l’altro: cura gli adempimenti istruttori relativi all’esercizio delle funzioni del Presidente del Consiglio dei ministri in tema di segreto di Stato; predispone le misure volte a garantire la sicurezza delle informazioni classificate ed effettua ispezioni e verifiche in materia presso pubbliche amministrazioni, enti pubblici e privati ed operatori economici abilitati; è l’Ufficio di riferimento per le **abilitazioni di sicurezza**; predispone e negozia gli **accordi di sicurezza**.

Il dirigente è nominato e revocato dal Presidente del Consiglio dei ministri, su proposta dell’Autorità delegata, ove istituita, sentito il Direttore generale del Dipartimento delle informazioni per la sicurezza.

UFFICIO INVENTARIO

Struttura costituita nell’ambito dell’Ufficio Centrale per la Segretezza presso cui confluiscono i dati identificativi dei segreti di Stato. L’elenco aggiornato dei segreti di Stato viene comunicato al COPASIR dal Presidente del Consiglio dei ministri nell’ambito della **Relazione sull’attività dei servizi di informazione**.

V

VALUTAZIONE

Termine che indica due distinte attività della fase di **elaborazione**. L'una consistente nell'esaminare il grado di fondatezza di una notizia ed il livello di affidabilità della fonte che la ha fornita. In proposito, presso i servizi di informazione occidentali è consolidato il ricorso ad una "matrice" che – al fine di mettere il destinatario in condizione di apprezzare il "peso specifico" dell'apporto informativo fornitogli – classifica l'attendibilità della fonte con lettere maiuscole da "A" ad "F" (A: affidabile, la fonte ha dimostrato di essere credibile e competente; B: normalmente affidabile; C: abbastanza affidabile, esistono dei dubbi sulla piena credibilità della fonte che ha peraltro fornito notizie rivelatesi corrispondenti al vero; D: usualmente non affidabile, sebbene abbia fornito sporadicamente notizie fondate; F: non classificabile) e la fondatezza della notizia con numeri arabi da "1" a "6" (1. notizia confermata, poiché riscontrata da altre fonti, logica e coerente con il patrimonio informativo sul soggetto o sul tema; 2. probabilmente vera: sebbene non confermata, la notizia appare logica e coerente con il patrimonio informativo sul soggetto o sul tema; 3. possibilmente vera: la notizia, priva di conferma, risulta ragionevolmente logica e concorda con alcuni elementi informativi già disponibili; 4. di dubbia fondatezza: la notizia, non confermata, appare possibile ma non logica e non trova riscontro in altri elementi informativi; 5. improbabile: la notizia non appare logica ed è contraddetta da altre informazioni; 6. non classificabile). In tale contesto

massima attendibilità assume l'apporto informativo valutato "A1".

L'altra consistente nel combinare tutti i dati informativi in un giudizio unitario che include spesso la formulazione di ipotesi circa le più probabili linee di sviluppo di un fenomeno o di una situazione. Rientra in questo ambito anche la "valutazione della minaccia", tipica per esempio del settore del controterrorismo, che si sostanzia in un esame di tutte le informazioni disponibili su potenziali attività ostili – con peculiare riguardo a capacità ed intento delle organizzazioni terroristiche ed al loro *modus operandi* – finalizzato ad identificare la probabilità di attacchi ed i possibili obiettivi.

VARIABILI CHIAVE

Fattori ritenuti determinanti perché una situazione o un fenomeno oggetto di **monitoraggio informativo** evolvano in una specifica direzione. Qualora rilevati dalla ricerca informativa, concorrono a tracciare uno scenario previsionale.

VERIFICA AMBIENTALE

Complesso di operazioni finalizzate a rilevare la presenza di apparecchiature/sistemi di intercettazione.

VINCOLO DI NON DIVULGAZIONE

Limitazione della diffusione di informazioni oggetto di **scambio informativo**, nell'ambito della **collaborazione internazionale intelligence**, alle sole parti coinvolte o comunque ad un novero di soggetti espressamente indicato.

VIOLAZIONE DELLA SICUREZZA

Azione o omissione contraria alle disposizioni in materia di tutela delle informazioni classificate.

W

WARNING

Gergo mutuato dal contesto anglosassone, indica un **prodotto intelligence** con cui viene segnalato un pericolo imminente per la sicurezza nazionale.

INDICE ALFABETICO

A

ABILITAZIONE DI SICUREZZA
ABILITAZIONE PREVENTIVA
ACCESSO
ACCORDO DI COOPERAZIONE/COLLABORAZIONE
ACCORDO DI SICUREZZA
ACINT (ACOUSTICAL INTELLIGENCE)
ACQUISIZIONE INFORMATIVA
AFFIDABILITÀ
AGENTE
AGENTE DOPPIO
AGENTE DI INFLUENZA
AGENZIA INFORMAZIONI E SICUREZZA ESTERNA (AISE)
AGENZIA INFORMAZIONI E SICUREZZA INTERNA (AISI)
AGENZIA INTELLIGENCE
AGENZIA NAZIONALE DI DISTRIBUZIONE
AGENZIE
AISE
AISI
ALL-SOURCE INTELLIGENCE
ANALISI
ANALISI DELLE IPOTESI CONFLIGGENTI
ANALISI DEL RISCHIO
ANALISI SWOT
ANALISTA
ANS
ANTENNA
APPOSIZIONE DEL SEGRETO DI STATO
AREA CONTROLLATA
AREA DI INTERESSE
AREA RISERVATA
ATTENDIBILITÀ

ATTIVITÀ DI INFORMAZIONE PER LA SICUREZZA
ATTIVITÀ ECONOMICHE SIMULATE
ATTIVITÀ INFO-OPERATIVA
ATTIVITÀ INFORMATIVA
ATTIVITÀ INTELLIGENCE
AUTENTICAZIONE
AUTORITÀ DELEGATA
AUTORITÀ NAZIONALE PER LA SICUREZZA (ANS)
AUTORIZZAZIONE ALL'ACCESSO CIFRA

B

BONIFICA
BRUCIARE/BRUCIATURA

C

CARATTERISTICHE DEI PRODOTTI INTELLIGENCE
CASE OFFICER
CAVEAT
CELLULA DORMIENTE
CENTRO
CENTRO DI VALUTAZIONE
CERTIFICAZIONE
CICLO INTELLIGENCE
CIFRA
CIFRATURA
CISR
CLASSIFICA DI SEGRETEZZA
CLASSIFICAZIONE
CLASSIFICHE DI SEGRETEZZA INTERNAZIONALI E COMUNITARIE
CLAUSOLA CATCH-ALL
CODIFICA
COLLABORAZIONE INTERNAZIONALE INTELLIGENCE
COLLABORAZIONE ISTITUZIONALE
COLLAZIONE
COLLEGATO ESTERO

COMINT (COMMUNICATIONS INTELLIGENCE)
COMITATO DI ANALISI STRATEGICA ANTITERRORISMO (CASA)
COMITATO DI SICUREZZA FINANZIARIA (CSF)
COMITATO INTERMINISTERIALE PER LA SICUREZZA
DELLA REPUBBLICA (CISR)
COMITATO PARLAMENTARE PER LA SICUREZZA
DELLA REPUBBLICA (COPASIR)
COMPARTIMENTAZIONE
COMPARTO INFORMATIVO/INTELLIGENCE
COMPROMISSIONE
COMPUSEC (COMPUTER SECURITY)
COMSEC (COMMUNICATION SECURITY)
COMUNICAZIONE ISTITUZIONALE
COMUNITÀ INTELLIGENCE
CONFIDENTE
CONSIGLIO GENERALE PER LA LOTTA ALLA CRIMINALITÀ
ORGANIZZATA
CONTROINDICAZIONI
CONTROINFORMAZIONE
CONTROINGERENZA
CONTROLLO SUL SISTEMA DI INFORMAZIONE PER LA SICUREZZA
DELLA REPUBBLICA
CONTROPROLIFERAZIONE
CONTROPROPAGANDA
CONTROSPIONAGGIO
CONTROTERRORISMO
COOPERAZIONE INTERNAZIONALE INTELLIGENCE
COORDINAMENTO
COPASIR
COPERTURA
COPERTURA INFORMATIVA
COUNTERINTELLIGENCE
CRIMINALITÀ ORGANIZZATA
CRITTANALISI
CRITTOGRAFIA

CRITTOLOGIA
CULTURA DELLA SICUREZZA
CURRENT INTELLIGENCE
CYBER-DEFENCE
CYBER-INTELLIGENCE
CYBER-SECURITY
CYBER-SPACE
CYBER-THREAT
CYBER-WAR

D

DECIFRATURA
DECLASSIFICA
DECODIFICA
DECRIITAZIONE
DEQUALIFICA
DIPARTIMENTO DELLE INFORMAZIONI PER LA SICUREZZA (DIS)
DIS
DISCIPLINE INTELLIGENCE
DISINFORMAZIONE
DISPOSITIVO DI RICERCA
DISSEMINAZIONE
DOCUMENTI DI COPERTURA
DOCUMENTO CLASSIFICATO

E

ELABORAZIONE
ELINT (ELECTRONIC INTELLIGENCE)
ENTE DI CERTIFICAZIONE
EVERSIONE

F

FABBISOGNO INFORMATIVO
FIDUCIARIO

FONTE
FONTE APERTA
FONTE CHIUSA
FONTE CONFIDENZIALE
FONTE DOCUMENTALE
FONTE TECNICA
FONTE UMANA
FUNZIONARIO ALLA SICUREZZA

G

GARANZIE FUNZIONALI
GEOINT (GEOSPATIAL INTELLIGENCE)
GESTIONE DELLE FONTI
GESTORE (CASE OFFICER)
GREY LITERATURE
GROUPTHINK

H

HUMINT (HUMAN INTELLIGENCE)

I

IDENTITÀ DI COPERTURA
IMINT (IMAGERY INTELLIGENCE)
INDICATORI CHIAVE
INDICATORI D'ALLARME
INFILTRATO
INFLUENZA
INFORMATION ASSURANCE (IA)
INFORMATION WARFARE
INFORMATIVA
INFORMATORE
INFORMAZIONE
INFORMAZIONE CLASSIFICATA

INFORMAZIONI INTELLIGENCE
INFORMAZIONI NON CLASSIFICATE CONTROLLATE
INFORMAZIONI SENSIBILI
INFOSEC (INFORMATION SECURITY)
INFRASTRUTTURE CRITICHE
INGERENZA
INTEGRAZIONE
INTEGRITÀ
INTELLIGENCE
INTELLIGENCE AD IMMEDIATO IMPATTO OPERATIVO
INTELLIGENCE "CIRCOLARE"
INTELLIGENCE DI BASE
INTELLIGENCE ECONOMICO-FINANZIARIA
INTELLIGENCE GREZZA
INTELLIGENCE MILITARE
INTELLIGENCE OPERATIVA
INTELLIGENCE STRATEGICA
INTELLIGENCE TATTICA
INTELLIGENCE TECNICA
INTERCETTAZIONI PREVENTIVE
INTERPRETAZIONE
INTERVISTA
INTOSSICAZIONE

L

LETTERATURA GRIGIA
LISTA DI ACCESSO
LIVELLI DI SEGRETEZZA
LUOGHI DI INTERESSE PER LA SICUREZZA DELLA REPUBBLICA

M

MASINT (MEASUREMENT AND SIGNATURE INTELLIGENCE)
MATERIALE CRITTOGRAFICO
MATERIALI DUAL USE

MATERIALI E DOCUMENTAZIONE COMSEC
MEDINT (MEDICAL INTELLIGENCE)
MINACCIA
MINACCIA ASIMMETRICA
MINACCIA CBRN
MINACCIA CIBERNETICA
MINACCIA CONVENZIONALE
MINACCIA CRIMINALE
MINACCIA ECONOMICO-FINANZIARIA
MINACCIA EVERSIVA
MINACCIA NON CONVENZIONALE
MINACCIA TERRORISTICA
MINACCIA TRANSNAZIONALE
MISSIONE
MODELLO OPERATIVO
MONITORAGGIO INFORMATIVO

N

NECESSITÀ DI CONOSCERE
NEED TO KNOW
NOS
NOTIZIE
NULLA OSTA DI SICUREZZA (NOS)
NULLA OSTA DI SICUREZZA INDUSTRIALE (NOSI)

O

OBIETTIVI INFORMATIVI
OBIETTIVO DI RICERCA
OMOLOGAZIONE
OPERAZIONE
OPERAZIONE SOTTO COPERTURA
OPPOSIZIONE DEL SEGRETO DI STATO
ORGANISMO INFORMATIVO
ORGANIZZAZIONE NAZIONALE PER LA SICUREZZA
OSINT (OPEN SOURCE INTELLIGENCE)

P

PATRIMONIO INFORMATIVO
PENETRAZIONE INFORMATIVA
PIANIFICAZIONE INFORMATIVA
PIANO DI RICERCA
PRESIDENTE DEL CONSIGLIO DEI MINISTRI
PROCESSO INFORMATIVO
PRODOTTI INTELLIGENCE
PRODUZIONE
PSYOPS (PSYCHOLOGICAL OPERATIONS)

Q

QUALIFICA DI SICUREZZA

R

RACCOLTA INFORMATIVA
REGOLA DELLA TERZA PARTE
RELAZIONE AL PARLAMENTO
RELAZIONE SULL'ATTIVITÀ DEI SERVIZI DI INFORMAZIONE
RICERCA INFORMATIVA
RIDUZIONE DELLA CLASSIFICA DI SEGRETEZZA
RISCHIO
RISERVATEZZA (OBBLIGO DI)
RISERVATISSIMO (RR)
RISERVATO (R)

S

SCAMBIO INFORMATIVO
SCUOLA DI FORMAZIONE DEL SISTEMA DI INFORMAZIONE
PER LA SICUREZZA DELLA REPUBBLICA
SEGRETERIA PRINCIPALE DI SICUREZZA
SEGRETEZZA (LIVELLI DI)
SEGRETISSIMO (SS)
SEGRETO (S)

SEGRETO DI STATO
SERVIZI
SERVIZIO COLLEGATO
SERVIZIO DI INFORMAZIONE
SICUREZZA CIBERNETICA
SICUREZZA CRITTOGRAFICA
SICUREZZA DELLE COMUNICAZIONI
SICUREZZA DELLE INFORMAZIONI
SICUREZZA FISICA
SICUREZZA INFORMATICA
SICUREZZA NAZIONALE
SIGINT (SIGNALS INTELLIGENCE)
SISTEMA DI INFORMAZIONE PER LA SICUREZZA
DELLA REPUBBLICA
SPIONAGGIO
STEGANOGRAFIA
STRUMENTI OPERATIVI

T

TEMPEST
TERRORISMO

U

UCSE
UFFICIALE ALLA SICUREZZA
UFFICIO CENTRALE DEGLI ARCHIVI
UFFICIO CENTRALE ISPETTIVO
UFFICIO CENTRALE PER LA SEGRETEZZA (UCSE)
UFFICIO INVENTARIO

V

VALUTAZIONE
VARIABILI CHIAVE

VERIFICA AMBIENTALE
VINCOLO DI NON DIVULGAZIONE
VIOLAZIONE DELLA SICUREZZA

W

WARNING

INDICE SISTEMATICO

STRUTTURE E ORGANI

AGENZIA INFORMAZIONI E SICUREZZA ESTERNA (AISE)
AGENZIA INFORMAZIONI E SICUREZZA INTERNA (AISI)
AGENZIA INTELLIGENCE
AGENZIA NAZIONALE DI DISTRIBUZIONE
AGENZIE
AISE
AISI
ANS
AUTORITÀ DELEGATA
AUTORITÀ NAZIONALE PER LA SICUREZZA (ANS)
CENTRO DI VALUTAZIONE
CISR
COLLEGATO ESTERO
COMITATO DI ANALISI STRATEGICA ANTITERRORISMO (CASA)
COMITATO DI SICUREZZA FINANZIARIA (CSF)
COMITATO INTERMINISTERIALE PER LA SICUREZZA
DELLA REPUBBLICA (CISR)
COMITATO PARLAMENTARE PER LA SICUREZZA
DELLA REPUBBLICA (COPASIR)
COMPARTO INFORMATIVO/INTELLIGENCE
COMUNITÀ INTELLIGENCE
CONSIGLIO GENERALE PER LA LOTTA ALLA CRIMINALITÀ
ORGANIZZATA
COPASIR
DIPARTIMENTO DELLE INFORMAZIONI PER LA SICUREZZA (DIS)
DIS
ENTE DI CERTIFICAZIONE
FUNZIONARIO ALLA SICUREZZA
ORGANISMO INFORMATIVO

ORGANIZZAZIONE NAZIONALE PER LA SICUREZZA
PRESIDENTE DEL CONSIGLIO DEI MINISTRI
SCUOLA DI FORMAZIONE DEL SISTEMA DI INFORMAZIONE PER
LA SICUREZZA DELLA REPUBBLICA
SEGRETERIA PRINCIPALE DI SICUREZZA
SERVIZI
SERVIZIO COLLEGATO
SERVIZIO DI INFORMAZIONE
SISTEMA DI INFORMAZIONE PER LA SICUREZZA
DELLA REPUBBLICA
UCSE
UFFICIALE ALLA SICUREZZA
UFFICIO CENTRALE DEGLI ARCHIVI
UFFICIO CENTRALE ISPETTIVO
UFFICIO CENTRALE PER LA SEGRETEZZA

ATTIVITÀ DI INFORMAZIONE PER LA SICUREZZA

DIREZIONE E CONTROLLO

AUTORITÀ DELEGATA
CISR
COMITATO INTERMINISTERIALE PER LA SICUREZZA
DELLA REPUBBLICA (CISR)
COMITATO PARLAMENTARE PER LA SICUREZZA
DELLA REPUBBLICA (COPASIR)
CONTROLLO SUL SISTEMA DI INFORMAZIONE
PER LA SICUREZZA DELLA REPUBBLICA
COORDINAMENTO
COPASIR
DIPARTIMENTO DELLE INFORMAZIONI PER LA SICUREZZA (DIS)
DIS
PRESIDENTE DEL CONSIGLIO DEI MINISTRI
RELAZIONE AL PARLAMENTO
RELAZIONE SULL'ATTIVITÀ DEI SERVIZI DI INFORMAZIONE
UFFICIO CENTRALE ISPETTIVO

CICLO INTELLIGENCE

ACQUISIZIONE INFORMATIVA

ALL-SOURCE INTELLIGENCE

ANALISI

ANALISI DELLE IPOTESI CONFLIGGENTI

ANALISI DEL RISCHIO

ANALISI SWOT

ANALISTA

ATTENDIBILITÀ

ATTIVITÀ DI INFORMAZIONE PER LA SICUREZZA

ATTIVITÀ INFO-OPERATIVA

ATTIVITÀ INFORMATIVA

ATTIVITÀ INTELLIGENCE

CARATTERISTICHE DEI PRODOTTI INTELLIGENCE

CICLO INTELLIGENCE

COLLAZIONE

COPERTURA INFORMATIVA

CURRENT INTELLIGENCE

DISSEMINAZIONE

ELABORAZIONE

FABBISOGNO INFORMATIVO

GROUPTHINK

INDICATORI CHIAVE

INDICATORI D'ALLARME

INFORMATIVA

INFORMAZIONE

INFORMAZIONI INTELLIGENCE

INTEGRAZIONE

INTELLIGENCE

INTELLIGENCE AD IMMEDIATO IMPATTO OPERATIVO

INTELLIGENCE "CIRCOLARE"

INTELLIGENCE DI BASE

INTELLIGENCE GREZZA

INTELLIGENCE OPERATIVA

INTELLIGENCE STRATEGICA

INTELLIGENCE TATTICA
INTERPRETAZIONE
MONITORAGGIO INFORMATIVO
NOTIZIE
OBIETTIVI INFORMATIVI
OBIETTIVO DI RICERCA
PATRIMONIO INFORMATIVO
PIANIFICAZIONE INFORMATIVA
PIANO DI RICERCA
PROCESSO INFORMATIVO
PRODOTTI INTELLIGENCE
PRODUZIONE
RACCOLTA INFORMATIVA
RICERCA INFORMATIVA
RISCHIO
VALUTAZIONE
VARIABILI CHIAVE
WARNING

DISCIPLINE ED AMBITI OPERATIVI

ACINT (ACOUSTICAL INTELLIGENCE)
AREA DI INTERESSE
COMINT (COMMUNICATIONS INTELLIGENCE)
COMUNICAZIONE ISTITUZIONALE
CONTROINFORMAZIONE
CONTROINGERENZA
CONTROPROLIFERAZIONE
CONTROPROPAGANDA
CONTROSPIONAGGIO
CONTROTERRORISMO
COUNTERINTELLIGENCE
CULTURA DELLA SICUREZZA
CYBER-DEFENCE
CYBER-INTELLIGENCE
CYBER-SECURITY
CYBER-SPACE

DISCIPLINE INTELLIGENCE
ELINT (ELECTRONIC INTELLIGENCE)
GEOINT (GEOSPATIAL INTELLIGENCE)
HUMINT (HUMAN INTELLIGENCE)
IMINT (IMAGERY INTELLIGENCE)
INFORMATION WARFARE
INFRASTRUTTURE CRITICHE
INTELLIGENCE ECONOMICO-FINANZIARIA
INTELLIGENCE MILITARE
INTELLIGENCE TECNICA
MASINT (MEASUREMENT AND SIGNATURE INTELLIGENCE)
MEDINT (MEDICAL INTELLIGENCE)
OSINT (OPEN SOURCE INTELLIGENCE)
SICUREZZA CIBERNETICA
SICUREZZA NAZIONALE
SIGINT (SIGNALS INTELLIGENCE)

STRUMENTI E MODALITÀ

ACCESSO
ACCORDO DI COOPERAZIONE/COLLABORAZIONE
AGENTE
AGENTE DI INFLUENZA
ANTENNA
ATTIVITÀ ECONOMICHE SIMULATE
BONIFICA
BRUCIARE/BRUCIATURA
CASE OFFICER
CAVEAT
CENTRO
CIFRA
CIFRATURA
CLAUSOLA CATCH-ALL
CODIFICA
COLLABORAZIONE INTERNAZIONALE INTELLIGENCE
COLLABORAZIONE ISTITUZIONALE
COMPARTIMENTAZIONE

CONFIDENTE
COOPERAZIONE INTERNAZIONALE INTELLIGENCE
COPERTURA
CRITTANALISI
CRITTOGRAFIA
CRITTOLOGIA
DECIFRATURA
DECODIFICA
DECRIITTAZIONE
DISPOSITIVO DI RICERCA
DOCUMENTI DI COPERTURA
FIDUCIARIO
FONTE
FONTE APERTA
FONTE CHIUSA
FONTE CONFIDENZIALE
FONTE DOCUMENTALE
FONTE TECNICA
FONTE UMANA
GARANZIE FUNZIONALI
GESTIONE DELLE FONTI
GESTORE (CASE OFFICER)
GREY LITERATURE
IDENTITÀ DI COPERTURA
INFILTRATO
INFORMATORE
INTERCETTAZIONI PREVENTIVE
INTERVISTA
LETTERATURA GRIGIA
MISSIONE
MODELLO OPERATIVO
NECESSITÀ DI CONOSCERE
NEED TO KNOW
OPERAZIONE
OPERAZIONE SOTTO COPERTURA
PENETRAZIONE INFORMATIVA

PSYOPS (PSYCHOLOGICAL OPERATIONS)
REGOLA DELLA TERZA PARTE
RISERVATEZZA (OBBLIGO DI)
SCAMBIO INFORMATIVO
STEGANOGRAFIA
STRUMENTI OPERATIVI
VERIFICA AMBIENTALE
VINCOLO DI NON DIVULGAZIONE

MINACCE

AGENTE DOPPIO
CELLULA DORMIENTE
COMPROMISSIONE
CRIMINALITÀ ORGANIZZATA
CYBER-THREAT
CYBER-WAR
DISINFORMAZIONE
EVERSIONE
INFLUENZA
INGERENZA
INTOSSICAZIONE
MATERIALI DUAL USE
MINACCIA
MINACCIA ASIMMETRICA
MINACCIA CBRN
MINACCIA CIBERNETICA
MINACCIA CONVENZIONALE
MINACCIA CRIMINALE
MINACCIA ECONOMICO-FINANZIARIA
MINACCIA EVERSIVA
MINACCIA NON CONVENZIONALE
MINACCIA TERRORISTICA
MINACCIA TRANSNAZIONALE
SPIONAGGIO
TERRORISMO

*TUTELA DELLE INFORMAZIONI CLASSIFICATE
E SEGRETO DI STATO*

AUTORITÀ E STRUTTURE

AGENZIA NAZIONALE DI DISTRIBUZIONE
ANS
AREA CONTROLLATA
AREA RISERVATA
AUTORITÀ NAZIONALE PER LA SICUREZZA (ANS)
CENTRO DI VALUTAZIONE
DIPARTIMENTO DELLE INFORMAZIONI PER LA SICUREZZA (DIS)
DIS
ENTE DI CERTIFICAZIONE
FUNZIONARIO ALLA SICUREZZA
LUOGHI DI INTERESSE PER LA SICUREZZA DELLA REPUBBLICA
ORGANIZZAZIONE NAZIONALE PER LA SICUREZZA
PRESIDENTE DEL CONSIGLIO DEI MINISTRI
SEGRETERIA PRINCIPALE DI SICUREZZA
UCSE
UFFICIALE ALLA SICUREZZA
UFFICIO CENTRALE PER LA SEGRETEZZA
UFFICIO INVENTARIO

ATTIVITÀ

ABILITAZIONE DI SICUREZZA
ABILITAZIONE PREVENTIVA
ACCESSO
ACCORDO DI SICUREZZA
AFFIDABILITÀ
APPOSIZIONE DEL SEGRETO DI STATO
AUTENTICAZIONE
AUTORIZZAZIONE ALL'ACCESSO CIFRA
CAVEAT
CERTIFICAZIONE
CIFRA
CIFRATURA

CLASSIFICA DI SEGRETEZZA
CLASSIFICAZIONE
CLASSIFICHE DI SEGRETEZZA INTERNAZIONALI E COMUNITARIE
CODIFICA
COMPROMISSIONE
COMPUSEC (COMPUTER SECURITY)
COMSEC (COMMUNICATION SECURITY)
CONTROINDICAZIONI
CRITTANALISI
CRITTOGRAFIA
CRITTOLOGIA
DECIFRATURA
DECLASSIFICA
DECODIFICA
DECRITTAZIONE
DEQUALIFICA
DOCUMENTO CLASSIFICATO
INFORMATION ASSURANCE (IA)
INFORMAZIONE CLASSIFICATA
INFORMAZIONI NON CLASSIFICATE CONTROLLATE
INFORMAZIONI SENSIBILI
INFOSEC (INFORMATION SECURITY)
INTEGRITÀ
LISTA DI ACCESSO
LIVELLI DI SEGRETEZZA
MATERIALE CRITTOGRAFICO
MATERIALI E DOCUMENTAZIONE COMSEC
NECESSITÀ DI CONOSCERE
NEED TO KNOW
NOS
NULLA OSTA DI SICUREZZA (NOS)
NULLA OSTA DI SICUREZZA INDUSTRIALE (NOSI)
OMOLOGAZIONE
OPPOSIZIONE DEL SEGRETO DI STATO
QUALIFICA DI SICUREZZA

RIDUZIONE DELLA CLASSIFICA DI SEGRETEZZA
RISERVATISSIMO (RR)
RISERVATO (R)
SEGRETEZZA (LIVELLI DI)
SEGRETISSIMO (SS)
SEGRETO (S)
SEGRETO DI STATO
SICUREZZA CRITTOGRAFICA
SICUREZZA DELLE COMUNICAZIONI
SICUREZZA DELLE INFORMAZIONI
SICUREZZA FISICA
SICUREZZA INFORMATICA
STEGANOGRAFIA
TEMPEST
VIOLAZIONE DELLA SICUREZZA

Edito da De Luca Editori Srl
Via di Novella, 22
00199 Roma

1ª ristampa aggiornata

Finito di stampare
nel mese di marzo 2013
Stampato in Italia - Printed in Italy
ISBN 978-88-6557-093-7