



OSSERVATORIO NAZIONALE SULLA PROLIFERAZIONE DELLE ARMI COGNITIVE

ONPAC-OLITEC

DOSSIER INFORMATIVO PER POTENZIALI COMPONENTI E COLLABORATORI

Scenario, missione, governance, metodo operativo e programma dei White Paper

Versione 1.1 – ottobre 2026

Inaugurazione istituzionale prevista: Gennaio 2027

DOCUMENTO INFORMATIVO PRELIMINARE

Destinato all'interlocuzione e alla valutazione di candidature. Non costituisce nomina, incarico, atto pubblico o documento operativo definitivo.

Nota sullo status del dossier

Finalità, base documentale e condizioni di utilizzo

Questo dossier è stato predisposto per consentire a persone potenzialmente interessate a entrare negli organi, nell'Unità Operativa, nella rete consultiva o nel sistema di revisione dell'ONPAC-OLITEC di comprendere prima della candidatura la natura dell'iniziativa, il contesto strategico nel quale nasce, le responsabilità connesse e il metodo di lavoro previsto. Non è un documento promozionale: è uno strumento di orientamento e di trasparenza preventiva, concepito per permettere una valutazione informata dell'impegno richiesto.

La base organizzativa è costituita dal "Programma istitutivo, regolamento e manuale operativo" dell'Osservatorio Nazionale sulla Proliferazione delle Armi Cognitive, versione 1.1 di luglio 2026. Tale testo ha natura di bozza tecnico-organizzativa e dovrà essere armonizzato, prima dell'adozione, con lo Statuto e il Regolamento generale della Fondazione, la disciplina in materia di protezione dei dati, le indicazioni del consulente legale, del responsabile della protezione dei dati e degli organi competenti. La denominazione "nazionale" individua il perimetro territoriale e conoscitivo dell'attività e non attribuisce all'Osservatorio natura pubblica né funzioni autoritative, investigative, militari, di intelligence o sanzionatorie.^[1]

Distinzione essenziale

L'inaugurazione istituzionale prevista per gennaio 2027 indica l'avvio pubblico dell'iniziativa e della fase di costituzione. La piena operatività tecnica sarà progressiva e potrà essere dichiarata soltanto dopo il completamento dei criteri di go-live: governance formalmente operativa, metodologia approvata, presidi privacy e sicurezza attivi, infrastruttura testata, procedure di replica e correzione pubblicate e personale adeguatamente formato.^[1]

Voce	Precisazione
Destinatari	Potenziati componenti dei comitati, candidati alle funzioni direttive e operative, revisori esterni, partner scientifici e professionali, referenti della rete consultiva e territoriale.
Uso previsto	Valutazione preliminare dell'adesione; base per colloqui, manifestazioni di interesse, dichiarazioni di disponibilità e successivi atti formali.
Cosa non produce	Nessuna nomina, autorizzazione, delega a rappresentare la Fondazione, accesso a dati o casi, vincolo contrattuale o riconoscimento di una qualifica pubblica.
Criterio di lettura	Le affermazioni di scenario sono accompagnate da fonti ufficiali; le valutazioni sull'Italia sono presentate come analisi di rischio, non come giudizi assoluti o attribuzioni di responsabilità.

Premessa

Proteggere la libertà di comprendere, scegliere e partecipare

Stiamo entrando in una fase nella quale la qualità della sicurezza di un Paese dipende non soltanto dalla protezione delle sue infrastrutture materiali e digitali, ma dalla capacità delle persone, delle istituzioni e delle organizzazioni di mantenere lucidità, fiducia e autonomia decisionale in un ambiente informativo sempre più artificiale, personalizzato e contestabile.

La guerra cognitiva non è un'espressione destinata a sostituire indiscriminatamente parole come propaganda, disinformazione o persuasione. È il nome di una trasformazione più profonda: la convergenza tra intelligenza artificiale generativa, profilazione comportamentale, automazione delle comunicazioni, reti coordinate, ambienti immersivi, dati biometrici e sistemi decisionali rende possibile intervenire non soltanto sulle informazioni che raggiungono una persona, ma sui processi attraverso i quali quella persona attribuisce significato, riconosce una fonte, costruisce fiducia, forma un giudizio e decide come agire. Quando tali capacità vengono impiegate con inganno, occultamento, coercizione o sfruttamento sistematico delle vulnerabilità, il bersaglio non è più soltanto il contenuto di una conversazione: è la libertà mentale che rende possibile la vita democratica.^[1, 2, 3]

L'Italia non è priva di competenze né di istituzioni capaci di affrontare parti rilevanti del problema. Possiede centri di ricerca, autorità, apparati di sicurezza, università, imprese e professionisti di alto livello. Tuttavia, il fenomeno attraversa contemporaneamente cybersicurezza, informazione, salute, protezione dei dati, istruzione, economia, processi democratici e difesa. Proprio perché nessun singolo settore può leggerlo interamente, il rischio più concreto è la frammentazione: segnali significativi possono rimanere separati, le evidenze non diventare comparabili e la risposta arrivare quando l'effetto cognitivo si è già consolidato. L'Osservatorio nasce per contribuire a colmare questo spazio di raccordo, senza sostituirsi alle autorità e senza trasformare il dissenso in una questione di sicurezza.

La Fondazione OLITEC assume questa iniziativa come un impegno di lungo periodo. Le competenze maturate nelle discipline BRIA – Bioinformatica, Realtà Immersiva e Intelligenza Artificiale – saranno messe al servizio di un presidio civile, scientifico e indipendente, orientato alla ricerca applicata, al monitoraggio, alla formazione e alla rendicontazione pubblica. L'obiettivo non sarà produrre allarme, ma conoscenza verificabile; non cercare colpevoli in assenza di prove, ma distinguere capacità, indicatori, incidenti, campagne e attacchi; non giudicare opinioni, ma analizzare comportamenti, tecniche, coordinamento, scala ed effetti.

A chi riceve questo dossier chiediamo quindi di valutare l'eventuale partecipazione con serietà. Entrare nell'ONPAC-OLITEC non dovrà essere un'adesione simbolica né un titolo onorifico. Significherà accettare regole di indipendenza, dichiarare i conflitti di interesse, proteggere le fonti, lavorare con dati incompleti senza colmare i vuoti con supposizioni, sottoporsi alla revisione dei pari e correggere pubblicamente gli errori quando emergano. Significherà anche contribuire a rendere comprensibili temi complessi a decisori, professionisti, militari, insegnanti, famiglie e cittadini che non possiedono una formazione tecnica specialistica.

Il risultato più visibile sarà la produzione di uno o più White Paper: un rapporto nazionale annuale e, quando necessario, approfondimenti tematici. La stessa base probatoria dovrà essere restituita in tre versioni differenziate: una destinata al Governo, alle istituzioni e ai decisori pubblici; una rivolta alle Forze Armate e agli organismi della difesa e della sicurezza; una accessibile ai cittadini, alle scuole, ai media e al tessuto produttivo. Le tre versioni non dovranno contenere verità differenti, ma livelli diversi di profondità, lessico e orientamento operativo, mantenendo identici criteri di prova, limiti e conclusioni.

Proteggere l'integrità cognitiva significa custodire la possibilità di comprendere, scegliere e partecipare liberamente alla vita collettiva. È una forma di sicurezza democratica e, nello stesso tempo, un dovere verso le generazioni che cresceranno in ambienti nei quali volti, voci, relazioni e interlocutori possono essere generati artificialmente. La credibilità dell'Osservatorio dipenderà dalla qualità delle persone che ne assumeranno la responsabilità, dalla prudenza delle conclusioni e dalla capacità di restare fedeli al metodo anche nei momenti di maggiore pressione.

Massimiliano Nicolini

Presidente Onorario della Fondazione Olivetti Tecnologia e Ricerca – OLITEC

Indice dei contenuti

Struttura del dossier e percorso di lettura

Sezione	Contenuto
Premessa	Il significato dell'iniziativa e l'impegno richiesto ai futuri componenti.
Sintesi esecutiva	Le ragioni, la missione, le garanzie e i risultati attesi.
1. Perché un Osservatorio sulle armi cognitive	La trasformazione della sicurezza e il nuovo spazio di rischio.
2. Scenario globale	Attori, tecnologie, tendenze e dati internazionali.
3. Scenario italiano	Punti di forza, vulnerabilità e necessità di raccordo nazionale.
4. Rischi per la società	Impatto su persone, famiglie, economia, servizi, democrazia e difesa.
5. Identità e mandato dell'ONPAC-OLITEC	Finalità, campo di osservazione, principi e attività escluse.
6. Governance e profili di coinvolgimento	Organi, ruoli, competenze e responsabilità dei candidati.
7. Metodo operativo	Segnalazione, triage, prova, rischio, confidenza, revisione e pubblicazione.
8. Programma dei White Paper	Una base probatoria comune e tre versioni distinte per i lettori.
9. Avvio, roadmap e criteri di maturità	Dall'inaugurazione di gennaio 2027 al pieno regime.
10. Impegno richiesto ai candidati	Indipendenza, riservatezza, formazione e disciplina scientifica.
Appendici	Tassonomia, matrice del rischio, glossario e fonti essenziali.

Percorso consigliato

Chi deve valutare rapidamente l'opportunità di aderire può leggere la Premessa, la Sintesi esecutiva, i capitoli 5, 6, 8 e 10. Chi è chiamato a contribuire alla metodologia dovrebbe approfondire anche i capitoli 2, 3, 4 e 7 e le appendici tecniche.

Sintesi esecutiva

Le informazioni essenziali per una valutazione consapevole

L'ONPAC-OLITEC è progettato come una struttura permanente di ricerca applicata, osservazione, valutazione e resilienza cognitiva. Il suo compito sarà comprendere come capacità tecnologiche e organizzative legittime o dual use possano essere trasformate in strumenti di manipolazione ad alto impatto, documentare gli impieghi rilevati nello spazio informativo italiano e produrre conoscenza utilizzabile senza invadere le competenze dello Stato.

Un rischio sistemico, non soltanto informativo

- 1 Le armi cognitive possono colpire percezione, attenzione, memoria, emozione, identità, fiducia e decisione. L'effetto può propagarsi dalla singola persona alle organizzazioni, ai mercati, ai processi democratici e alla sicurezza nazionale.

Una minaccia accelerata dall'intelligenza artificiale

- 2 L'IA riduce costi e tempi, aumenta la scala, consente traduzione, personalizzazione, clonazione di voce e immagini, automazione di reti e adattamento continuo dei messaggi. Il rapporto EEAS 2026 ha rilevato 147 incidenti FIMI con tecniche collegate all'IA nel 2025, contro 41 nel 2024.

Un'Italia dotata di risorse, ma preparata in modo diseguale

- 3 Il Paese dispone di forti basi industriali, ricerca, servizi pubblici digitali e istituzioni competenti. Persistono però divari nelle competenze digitali, scarsità di specialisti, dipendenza da piattaforme globali e frammentazione tra ambiti normativi e operativi.

Un osservatorio civile e non autoritativo

- 4 L'ONPAC non svolgerà funzioni di polizia, intelligence, censura, vigilanza o attribuzione giuridica. Analizzerà comportamenti e tecniche, non opinioni. Le sue conclusioni saranno scientifiche e documentali, sottoposte a revisione e diritto di replica.

Un metodo fondato su neutralità, prova e proporzionalità

- 5 Ogni affermazione pubblica dovrà rinviare a un fascicolo, a fonti tracciate, a un livello di confidenza e a una revisione indipendente. Il rischio sarà distinto dalla solidità delle prove. La pubblicazione dovrà ridurre il danno, non amplificarlo.

White Paper differenziati per tre comunità di lettori

- 6 La base probatoria comune sarà tradotta in una versione istituzionale e di policy, una versione per difesa e sicurezza e una versione civile e divulgativa. A esse potranno aggiungersi rapporti tematici, bollettini e un Rapporto zero sul primo anno di avvio.

Messaggio per il candidato

L'Osservatorio richiede persone capaci di operare tra discipline diverse, accettare il controllo reciproco, mantenere riservatezza, distinguere fatti e ipotesi e comunicare con chiarezza. La qualità dell'ONPAC non sarà misurata dal numero di soggetti "segnalati", ma dalla solidità del metodo, dalla tempestività delle correzioni e dall'utilità pubblica dei suoi prodotti.^[1]

1. Perché un Osservatorio sulle armi cognitive

Dalla protezione delle reti alla protezione dei processi di comprensione e decisione

La sicurezza contemporanea non può essere descritta soltanto attraverso confini, piattaforme informatiche e infrastrutture fisiche. Una società dipende anche da beni immateriali: fiducia, attenzione, memoria condivisa, autorevolezza delle fonti, capacità di deliberare e disponibilità a cooperare. Quando questi beni vengono degradati intenzionalmente, il Paese può apparire funzionante e nello stesso tempo perdere progressivamente la propria capacità di comprendere, coordinarsi e reagire.

La mente come infrastruttura critica

Una rete elettrica è critica perché dalla sua continuità dipendono servizi essenziali. Anche la qualità dei processi cognitivi collettivi è critica: una falsa comunicazione di emergenza può produrre panico, un audio clonato può autorizzare una frode, una rete coordinata può simulare consenso o ostilità, una base di conoscenza contaminata può alterare il lavoro di migliaia di persone. La specificità del rischio cognitivo è che l'obiettivo non coincide necessariamente con il dispositivo o con il dato; può essere il significato attribuito al dato, l'urgenza percepita, il livello di fiducia o la decisione che ne deriva.

Le operazioni più efficaci non richiedono sempre una falsità totale. Possono utilizzare materiali autentici selezionati, documenti veri privati del contesto, immagini reali abbinati a descrizioni fuorvianti, o informazioni contraddittorie diffuse in quantità tale da rendere difficile ogni verifica. Il successo può consistere non nel far credere a tutti la stessa cosa, ma nel rendere impossibile stabilire criteri condivisi di autenticità. In questo senso, la confusione può essere un risultato strategico quanto la persuasione.

Che cosa si intende per “arma cognitiva”

Nel modello ONPAC la parola “arma” ha un significato funzionale, non ontologico. Nessuna piattaforma, tecnologia, applicazione o tecnica di comunicazione è un’arma per la sua sola esistenza. La qualifica dipende dal modo in cui viene utilizzata, dall'intenzionalità o dall'adattamento operativo, dalla presenza di inganno, occultamento o coercizione, dalla vulnerabilità dei bersagli, dalla scala e dal danno significativo effettivo o prevedibile. Questa prudenza terminologica è indispensabile per non criminalizzare l'innovazione, la persuasione legittima, il giornalismo, la satira, il dibattito politico o l'uso ordinario dell'intelligenza artificiale.^[1]

Definizione operativa ONPAC-OLITEC

Sistema, applicazione, servizio, interfaccia, contenuto, infrastruttura o processo uomo-macchina impiegato intenzionalmente, coordinato o adattato per alterare, inibire, frammentare, sfruttare o degradare percezione, attenzione, memoria, emozione, identità, giudizio, fiducia o capacità decisionale mediante tecniche ingannevoli, occulte, coercitive, discriminatorie o sproporzionate, con danno significativo effettivo o ragionevolmente prevedibile.^[1]

Termini vicini, ma non equivalenti

Concetto	Significato nel dossier
Disinformazione	Contenuto falso o fuorviante diffuso intenzionalmente. È una possibile tecnica, ma non esaurisce il fenomeno.
FIMI	Comportamento manipolativo intenzionale e coordinato, spesso riconducibile ad attori statali, non statali o proxy, capace di danneggiare valori e processi politici. Può essere in larga parte non illegale.
Operazione di influenza	Attività pianificata per orientare percezioni o comportamenti. Può essere lecita o illecita, trasparente o occulta; il contesto è decisivo.
Guerra cognitiva	Impiego sistematico di capacità informative, tecnologiche, psicologiche e organizzative per incidere sulla razionalità, sulla percezione e sul processo decisionale di persone e sistemi sociali.
Arma cognitiva	Qualificazione funzionale dello strumento o del processo concretamente impiegato in modo manipolativo o coercitivo, con danno significativo.

Concetto	Significato nel dossier
Resilienza cognitiva	Capacità individuale e collettiva di riconoscere pressioni manipolative, mantenere qualità decisionale, correggere gli errori e recuperare fiducia senza comprimere pluralismo e libertà.

Perché un presidio permanente

Le campagne cognitive sono cumulative e adattive. Possono svilupparsi per mesi, cambiare canale, riutilizzare infrastrutture precedenti, modificare i messaggi in base alle reazioni e sfruttare eventi futuri. Un'osservazione occasionale tende a vedere soltanto il contenuto virale del momento; un presidio permanente può invece confrontare cronologie, asset, tecniche, livelli di automazione, settori colpiti e contromisure. La continuità permette inoltre di distinguere l'aumento reale del fenomeno dall'aumento della capacità di rilevazione, evitando statistiche allarmistiche o interpretazioni basate su campioni non rappresentativi.

2. Scenario globale

La convergenza tra competizione strategica, piattaforme digitali e intelligenza artificiale

A livello globale la manipolazione dell'ambiente informativo è sempre più integrata con strumenti cyber, pressioni economiche, attività diplomatiche, operazioni militari, reti criminali e servizi commerciali di influenza. La novità non è l'esistenza della propaganda, ma la capacità di produrre, distribuire e adattare contenuti in modo continuo, multimodale e misurabile, sfruttando infrastrutture globali e vulnerabilità locali.

Il riconoscimento del dominio cognitivo

Nel giugno 2026 il NATO Defense College ha riunito a Roma 108 partecipanti provenienti da 67 istituzioni di formazione della difesa, rappresentative di 25 Paesi alleati e 20 partner, attorno al tema "The Mind as a Battlespace". Il confronto ha evidenziato che nelle operazioni cognitive il cervello umano può diventare sia bersaglio sia vettore: attori ostili cercano di intervenire su razionalità, percezioni e processi decisionali, sfruttando vulnerabilità cognitive e indebolendo la fiducia pubblica. La risposta indicata non si limita alla comunicazione strategica, ma include educazione, pensiero critico, salute mentale, capacità di operare nell'incertezza e protezione delle decisioni. ^[2, 3]

Il quadro NATO è rilevante anche per una struttura civile perché mostra che la resilienza non può essere confinata alle organizzazioni militari. Decisioni pubbliche, catene di comando, famiglie, imprese e media condividono lo stesso ambiente digitale. La pressione cognitiva può quindi attraversare il confine tra pace, crisi e conflitto, senza produrre sempre una soglia facilmente riconoscibile. Questo carattere persistente e ambiguo rende essenziale la cooperazione tra competenze tecniche, sociali, giuridiche, educative e di sicurezza.

Le dimensioni osservate dall'Unione europea

Il quarto rapporto annuale del Servizio europeo per l'azione esterna sulle minacce FIMI, pubblicato nel marzo 2026, descrive un ambiente nel quale le operazioni sono più frequenti, sofisticate, coordinate e intrecciate con il dominio cyber e fisico. Nel campione analizzato per il 2025, l'EEAS ha rilevato 540 incidenti globali, coinvolgendo 10.500 canali e siti. Più di cento Paesi, circa duecento organizzazioni e numerose personalità pubbliche sono stati presi di mira. Il 29% degli incidenti del campione è stato attribuito alla Russia, il 6% alla Cina; il restante 65% non è stato attribuito, pur presentando indicatori di coordinamento con infrastrutture note. Questi dati descrivono l'attività osservata e non devono essere interpretati come una misura completa della prevalenza globale. ^[4]

540	10.500	>100	27%
incidenti FIMI rilevati e analizzati nel 2025	canali, account, siti o blog coinvolti	Paesi interessati nel perimetro di osservazione	incidenti con tecniche collegate all'intelligenza artificiale

Indicatori del campione EEAS 2025. I numeri rappresentano casi osservati e analizzati, non una stima esaustiva del fenomeno mondiale. Fonte: EEAS, 4th Annual Report on FIMI Threats, 2026.

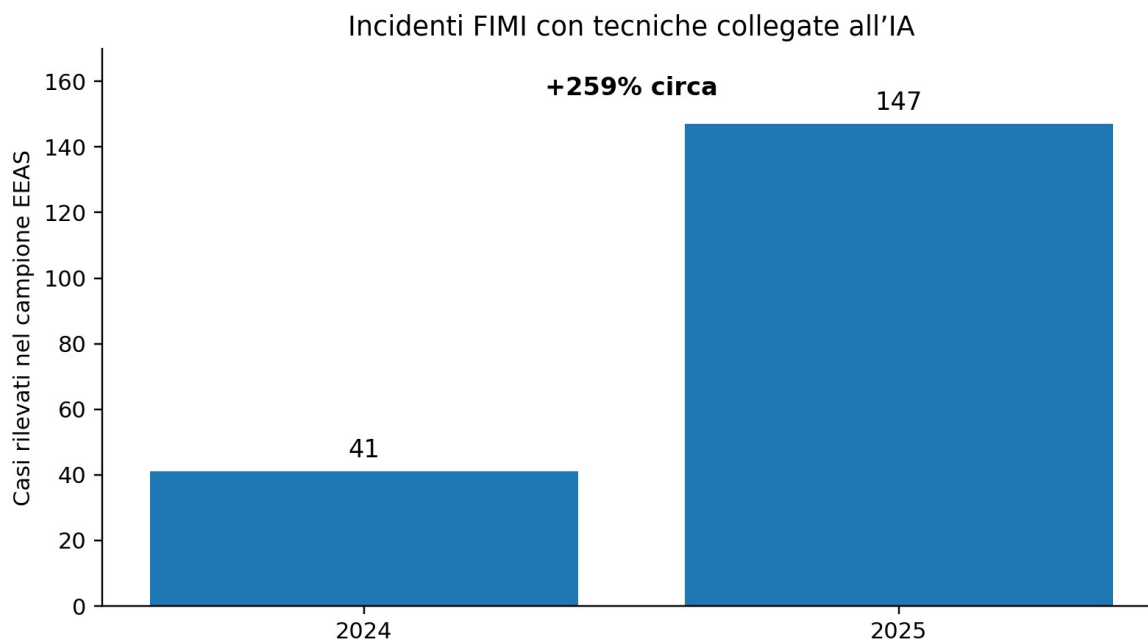


Figura 1 – Incidenti FIMI con tecniche collegate all'IA nel campione EEAS: da 41 nel 2024 a 147 nel 2025. Fonte: EEAS, 2026.

Perché l'intelligenza artificiale cambia la scala

L'intelligenza artificiale abbassa le barriere di ingresso e rende possibile una combinazione prima difficilmente sostenibile: produzione rapida, traduzione multilingue, adattamento al pubblico, clonazione di voce e immagine, creazione di identità coerenti, automazione della distribuzione e analisi delle reazioni. Il rapporto EEAS rileva che testo sintetico, audio artificiale e video manipolati sono passati dall'uso sperimentale a un impiego routinario e a basso costo. La quantità non implica necessariamente efficacia, ma aumenta la pressione sui verificatori e consente di occupare stabilmente lo spazio informativo con versioni reiterate e varianti locali.^[4]

Un ulteriore rischio riguarda la contaminazione delle fonti utilizzate dai sistemi di intelligenza artificiale. Reti di siti e contenuti di bassa qualità possono essere prodotte in più lingue per influenzare i risultati di ricerca, alimentare basi di conoscenza o comparire come fonti apparentemente indipendenti. Se un modello recupera, riassume o apprende da un ambiente già manipolato, la falsificazione non resta confinata al contenuto iniziale: può essere riutilizzata in risposte successive, report, materiali didattici e sistemi di supporto alle decisioni. Questa forma di "inquinamento cognitivo" ha una persistenza superiore al singolo post virale.

Attori e motivazioni

Categoria	Possibili finalità
Attori statali e proxy	Orientare scelte strategiche, indebolire alleanze, condizionare elezioni, giustificare azioni, erodere la fiducia.
Servizi commerciali di influenza	Offrire produzione, amplificazione, targeting o reputazione artificiale a clienti pubblici o privati.
Reti criminali	Frodi, estorsioni, furto d'identità, manipolazione di mercati, ricatti e monetizzazione dell'attenzione.
Gruppi estremisti o violenti	Reclutamento, radicalizzazione, intimidazione, polarizzazione e legittimazione della violenza.
Attori politici o economici opportunisti	Vantaggi elettorali, competitivi o reputazionali attraverso pratiche opache o coordinate.
Sistemi autonomi mal configurati	Danno non necessariamente intenzionale prodotto da ottimizzazioni, bias, feedback e incentivi non governati.

La catena tipica di un'operazione cognitiva

Fase	Funzione
1. Ricognizione	Individuazione di tensioni, vulnerabilità, eventi e pubblici.
2. Preparazione	Costruzione di asset, identità, canali e reputazione.
3. Produzione	Creazione o selezione di contenuti, documenti, voci, immagini e narrazioni.
4. Targeting	Scelta dei gruppi, dei momenti e dei fattori emotivi o decisionali.
5. Diffusione	Pubblicazione, pubblicità, messaggistica, reti coordinate e ricircolo.
6. Amplificazione	Simulazione di consenso, sincronizzazione, passaggio tra piattaforme.
7. Adattamento	Misurazione delle reazioni e modifica della strategia.
8. Persistenza	Contaminazione di archivi, motori di ricerca, memoria pubblica e sistemi IA.

Una cautela metodologica

Non ogni contenuto falso è una campagna, non ogni campagna è un attacco cognitivo e non ogni effetto osservato dimostra l'intenzione dell'autore. L'analisi deve separare contenuto, comportamento, diffusione, impatto e attribuzione. Beneficio politico o compatibilità narrativa non provano il controllo dell'operazione. ^[1, 4]

3. Scenario italiano

Un Paese con importanti capacità, ma una resilienza distribuita in modo diseguale

Definire l'Italia "debole" senza precisazioni sarebbe impreciso. Il Paese ha compiuto progressi rilevanti nella digitalizzazione, dispone di servizi pubblici digitali avanzati, di una solida base industriale e di ricerca e di competenze strategiche nei semiconduttori, nel calcolo ad alte prestazioni e nelle tecnologie quantistiche. La vulnerabilità riguarda soprattutto il divario tra la velocità della trasformazione e la capacità di integrare competenze, dati, formazione e risposta su scala nazionale.

Punti di forza da valorizzare

La Relazione italiana sul Decennio digitale 2026 riconosce progressi nell'FTTP, nella digitalizzazione delle piccole e medie imprese e nell'adozione di cloud, intelligenza artificiale e analisi dei dati. Evidenzia inoltre la qualità delle basi industriali e scientifiche e lo sviluppo dei servizi pubblici digitali, inclusi identità e sanità digitale. Questi elementi costituiscono una base favorevole per costruire resilienza: reti di ricerca, competenze pubbliche, capacità industriale e servizi digitali possono diventare partner di osservazione, formazione e risposta. ^[10]

Competenze digitali: il divario strutturale

Nel 2025 il 54,3% delle persone tra 16 e 74 anni possedeva competenze digitali almeno di base. Il dato è in crescita, ma resta 6,1 punti sotto la media dell'Unione europea e lontano dall'obiettivo dell'80% fissato per il 2030. La competenza digitale non coincide con la resilienza cognitiva, ma ne costituisce una condizione importante: chi non comprende come funzionano profilazione, raccomandazione, pubblicità, autenticazione o protezione dei dati ha maggiori difficoltà a riconoscere la manipolazione o a reagire in modo proporzionato. ^[9, 10]

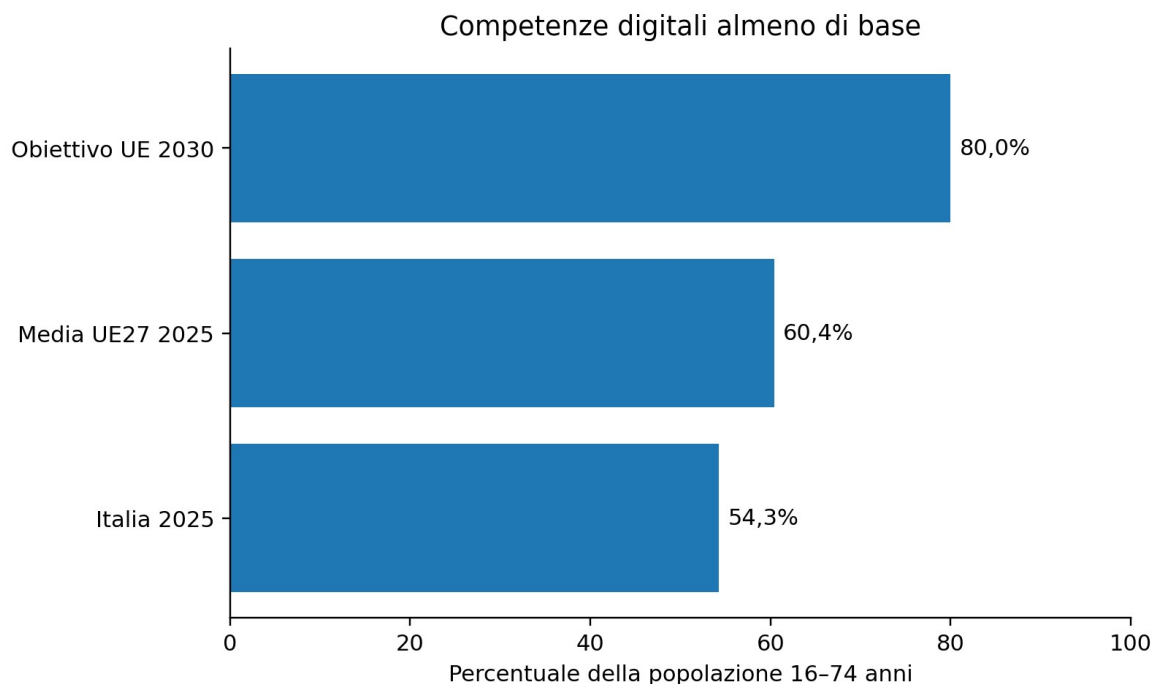


Figura 2 - Competenze digitali almeno di base. La media UE27 è ricavata dal divario di 6,1 punti indicato da ISTAT. Fonti: ISTAT, 2026; obiettivo UE 2030.

Le differenze interne sono altrettanto rilevanti. Tra i giovani di 20-24 anni che hanno utilizzato Internet negli ultimi tre mesi, il 71,7% possiede competenze almeno di base; la quota scende al 49,1% tra 55 e 59 anni e al 27,4% tra 65 e 74 anni. Il Mezzogiorno presenta inoltre un ritardo di circa cinque punti nell'accesso domestico a Internet rispetto al Centro-Nord. Queste differenze non devono essere trasformate in etichette di vulnerabilità personale, ma indicano la necessità di strumenti formativi differenziati per età, territorio e contesto sociale.^[9]

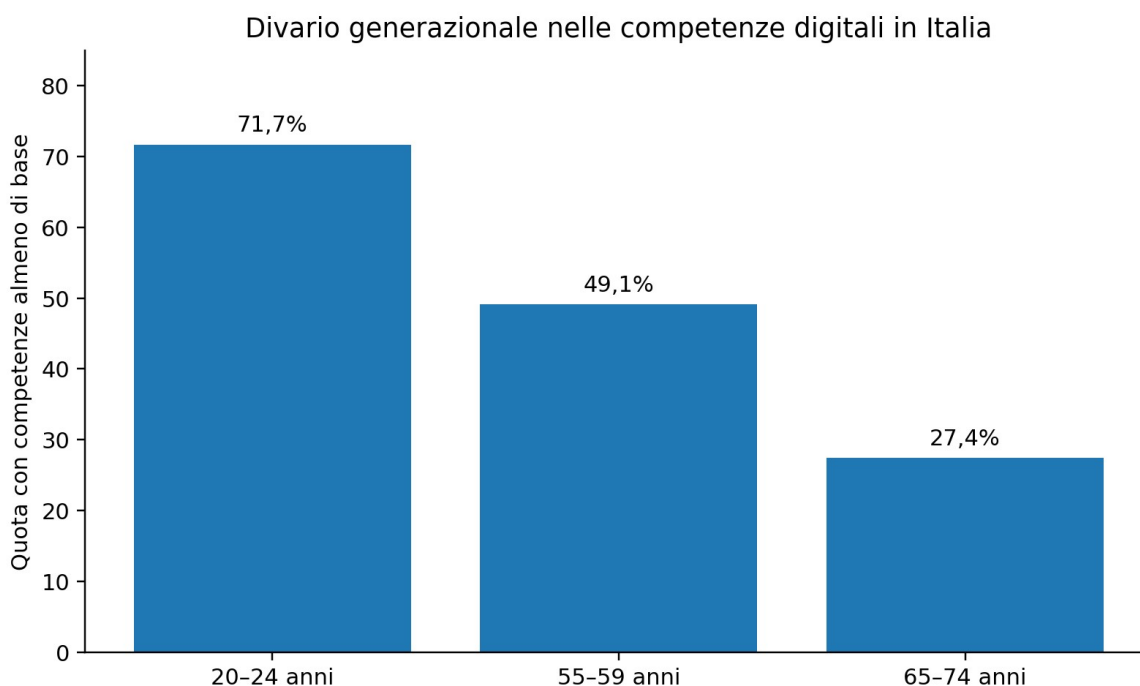


Figura 3 - Divario generazionale nelle competenze digitali almeno di base. Fonte: ISTAT, Cittadini e ICT - 2025.

La trasformazione dell'accesso all'informazione

Nel primo semestre del 2025 Internet rappresentava la prima porta di accesso all'informazione per il 55,8% degli italiani, mentre la televisione scendeva al 43,2%. Il passaggio non è negativo in sé: amplia le fonti, riduce le barriere e accelera la circolazione delle conoscenze. Tuttavia, sposta una parte crescente della formazione dell'opinione pubblica in ambienti organizzati da algoritmi di ranking e raccomandazione, pubblicità personalizzata, metriche di coinvolgimento e sistemi di profilazione che l'utente raramente vede o controlla.^[8]

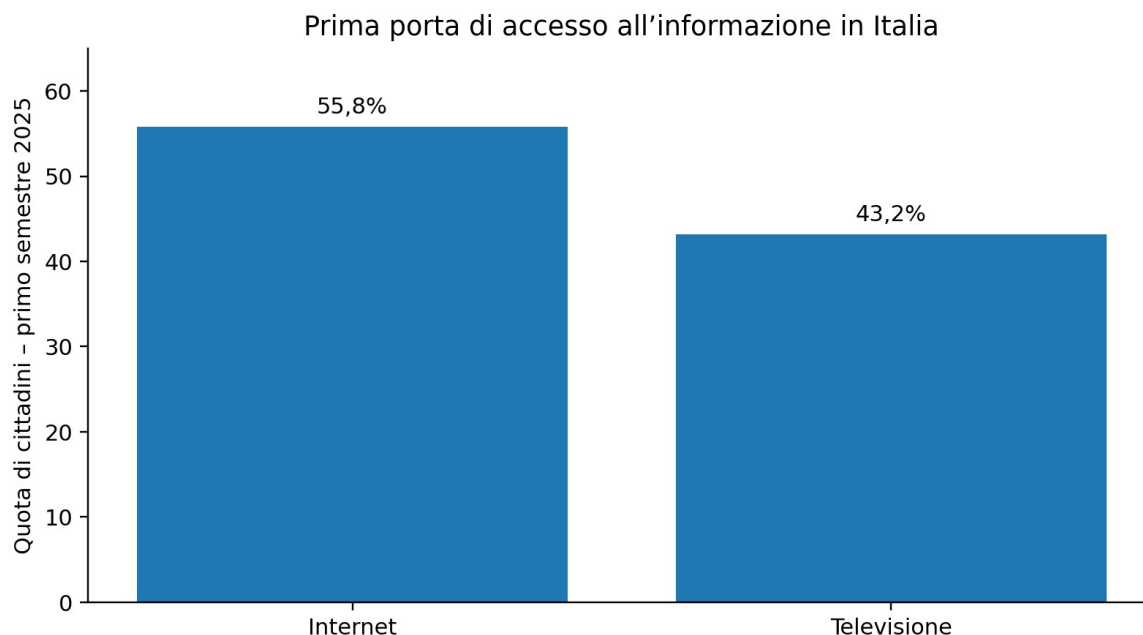


Figura 4 – Prima porta di accesso all'informazione in Italia, primo semestre 2025. Fonte: AGCOM, Osservatorio annuale sul sistema dell'informazione – II edizione, 2026.

La crescente centralità dell'online aumenta l'importanza della trasparenza delle piattaforme e dell'autenticità dei contenuti. Quando una narrativa viene artificialmente amplificata, il cittadino può scambiare per consenso spontaneo; quando una stessa falsificazione compare su siti diversi, può apparire corroborata; quando un contenuto è personalizzato sulla base di dati comportamentali, persone differenti possono ricevere versioni incompatibili senza poterle confrontare. L'AGCOM ha inoltre sottolineato nel Rapporto sull'intelligenza artificiale 2026 le questioni aperte relative a modelli generativi, trasparenza, diritti fondamentali, concorrenza e governance, confermando che il problema richiede competenze tecniche e regolatorie integrate.^[7, 8]

Le vulnerabilità di sistema

Area	Implicazione
Frammentazione istituzionale	La minaccia attraversa sicurezza, dati, media, salute, scuola, economia e processi democratici; i segnali possono restare separati tra competenze legittimamente diverse.
Dipendenza da ecosistemi globali	Piattaforme, modelli e infrastrutture decisive operano spesso fuori dal controllo nazionale e modificano rapidamente policy e accesso ai dati.
Divari di competenze	Differenze generazionali, territoriali e professionali riducono la capacità uniforme di riconoscere e segnalare fenomeni complessi.
Tessuto di PMI e amministrazioni locali	Molti soggetti dispongono di risorse limitate per forensics, comunicazione di crisi e formazione contro impersonificazione e frodi persuasive.
Polarizzazione e sfiducia	Narrative ostili possono sfruttare conflitti reali, senza dover inventare interamente il problema, rendendo più difficile la risposta comune.
Scarsa base dati comparabile	Senza tassonomia e registri condivisi è difficile distinguere crescita reale, crescita della rilevazione, falsi positivi e impatto misurato.

Una valutazione equilibrata

L'Italia non è indifesa; è preparata in modo diseguale. La risposta non richiede la creazione di un centro che assorba o replichi le funzioni di autorità, intelligence, forze di polizia o difesa. Richiede un'infrastruttura civile della conoscenza capace di osservare fenomeni trasversali, documentare il livello di prova, produrre indicatori comparabili, trasferire tempestivamente i casi alle competenze istituzionali e trasformare l'esperienza in formazione pubblica. L'ONPAC si colloca in questo spazio complementare.

La debolezza più profonda

Il rischio nazionale non consiste soltanto nell'adesione a una singola falsità. Consiste nella progressiva difficoltà di distinguere l'autentico dal costruito e nel deterioramento dei criteri condivisi con cui cittadini, istituzioni e organizzazioni verificano i fatti. Quando la sfiducia diventa generalizzata, anche le comunicazioni corrette perdono efficacia.^[1]

4. Rischi per la società

Dalla persona alla sicurezza nazionale: una catena di effetti interdipendenti

Le armi cognitive producono rischi a più livelli. Un danno individuale può propagarsi alla famiglia, all'impresa o al servizio pubblico; una manipolazione diffusa può invece iniziare come fenomeno collettivo e tradursi in decisioni personali. Per questo l'ONPAC valuterà separatamente gravità, portata, vulnerabilità del bersaglio, intensità manipolativa, coordinamento, persistenza e sensibilità strategica del momento.

Livello individuale: autonomia, identità e decisione

La persona può essere colpita attraverso impersonificazione, clonazione vocale, falsi documenti, relazioni artificiali persistenti, pressione emotiva e personalizzazione occulta. Il danno può essere economico, reputazionale, psicologico o fisico. Una chiamata che riproduce la voce di un familiare può indurre un pagamento urgente; un falso professionista sanitario può orientare una scelta pericolosa; un agente conversazionale può utilizzare memoria e conoscenza delle fragilità per rendere la persuasione progressivamente più efficace. La tutela non consiste nel diagnosticare la persona o sorvegliarne le opinioni, ma nel riconoscere le tecniche e ridurre la capacità dell'attore di sfruttare vulnerabilità non consapevoli.

Famiglie, minori e gruppi vulnerabili

I minori sono esposti a forme specifiche di rischio: deepfake sessuali, impersonificazione di coetanei o adulti, grooming, design compulsivo, ricatti, isolamento e dipendenza da interlocutori artificiali. Anche anziani, persone in condizioni di fragilità, soggetti sotto stress o con ridotta familiarità digitale possono essere presi di mira. Il criterio non deve diventare una classificazione stigmatizzante: la vulnerabilità è spesso situazionale e può riguardare chiunque durante una crisi, una perdita, una malattia o una decisione urgente.

Comunità e coesione sociale

A livello comunitario la manipolazione può amplificare fratture reali, simulare consenso, produrre ostilità tra gruppi o rendere impossibile il confronto. Reti di account coordinati possono far apparire una posizione marginale come dominante; contenuti emotivi possono essere distribuiti selettivamente a pubblici diversi; un incidente locale può essere decontestualizzato e trasformato in prova di una minaccia generale. L'effetto più grave non è sempre la polarizzazione visibile, ma l'erosione lenta della fiducia reciproca e della disponibilità a verificare prima di reagire.

Economia, imprese e lavoro

Imprese e professionisti possono subire frodi basate sulla voce o sul volto di dirigenti, falsi comunicati, campagne reputazionali, manipolazione di recensioni e indicatori, furto di identità, leak alterati o attacchi alla catena decisionale. Per una piccola impresa, la verifica forense e la comunicazione di crisi possono avere costi sproporzionati; per un'azienda quotata, una falsa informazione credibile può incidere su mercato, fornitori e personale prima che arrivi la smentita. Il rischio cognitivo si salda quindi al cyber risk, alla continuità operativa e alla governance dei dati.

Salute, emergenze e servizi essenziali

Durante emergenze sanitarie, ambientali o di protezione civile il tempo decisionale si riduce e la vulnerabilità aumenta. L'impersonificazione di un'autorità, false istruzioni di servizio, mappe alterate, allarmi sintetici o messaggi coordinati possono produrre panico, ostacolare le cure, sovraccaricare i canali ufficiali o indirizzare le persone verso condotte rischiose. In questi casi la risposta deve essere rapidissima ma anche prudente: ripetere dettagli nocivi o titoli falsi può amplificarli. L'Osservatorio dovrà privilegiare la correzione autorevole, il contatto con le autorità competenti e la minimizzazione della riproduzione del contenuto.

Democrazia e processi elettorali

Una campagna elettorale può essere colpita con deepfake di candidati, false informazioni di servizio, micro-targeting non trasparente, account coordinati, pubblicazione di materiali sottratti e alterati o tentativi di delegittimare l'intero processo di voto. L'obiettivo può essere il sostegno a un attore, ma anche l'astensione, la confusione, la contestazione preventiva del risultato o la rottura della fiducia nelle istituzioni. La valutazione deve essere simmetrica rispetto agli attori politici e non deve mai trasformarsi in un giudizio sulla legittimità di opinioni o programmi.

Difesa, sicurezza e capacità decisionale

Nel dominio della difesa il rischio riguarda la protezione delle decisioni, la coesione, la fiducia nella catena di comando, la percezione delle minacce e il rapporto tra Forze Armate e società. Una compromissione cyber può diventare vettore per un payload informativo; una comunicazione sintetica può imitare un'autorità; una narrativa coordinata può ridurre il sostegno a una missione o creare tensioni tra alleati. La resilienza cognitiva non richiede soltanto strumenti tecnici, ma formazione a riconoscere pressione, sovraccarico, urgenza artificiale, bias e fonti compromesse.

Conoscenza, ricerca e sistemi di intelligenza artificiale

La contaminazione di archivi, dataset, repository, motori di ricerca e basi di conoscenza può produrre effetti duraturi. Un contenuto manipolato, una volta indicizzato o riutilizzato da un modello, può ricomparire in report e decisioni successive. Il rischio è particolarmente elevato quando un sistema presenta una risposta con tono autorevole senza rendere visibile la provenienza o il livello di incertezza. L'Osservatorio dovrà quindi osservare non soltanto i messaggi rivolti al pubblico, ma anche i processi con cui informazioni e metriche entrano nei sistemi di supporto alle decisioni.

Mappa sintetica dei livelli di impatto

Livello	Possibili conseguenze	Esempi di vettori
Persona	Frode, identità, reputazione, salute, autonomia decisionale	Voci clonate, relazioni artificiali, targeting emotivo
Famiglia e gruppi vulnerabili	Ricatto, grooming, isolamento, panico, dipendenza	Deepfake, impersonificazione, design compulsivo
Comunità	Polarizzazione, ostilità, perdita di fiducia, conflitti locali	Amplificazione coordinata, consenso sintetico, decontestualizzazione
Impresa ed economia	Perdite, crisi reputazionale, decisioni alterate, continuità	Falsi dirigenti, leak manipolati, ranking e recensioni artificiali
Servizi pubblici e salute	Ostacolo alle cure, panico, sovraccarico, mancata risposta	Falsa autorità, istruzioni contraffatte, canali clonati
Democrazia	Sfiducia nel voto, astensione, delegittimazione, frammentazione	Deepfake, micro-targeting occulto, hacked-and-leaked
Difesa e sicurezza	Errore decisionale, perdita di coesione, indebolimento strategico	Cyber-cognitivo, impersonificazione, pressione informativa

Principio di proporzionalità

La comunicazione di un caso può essa stessa produrre danno, diffondere la falsità o esporre persone vulnerabili. Per questo l'ONPAC pubblicherà soltanto quando l'utilità di informare supera il rischio di amplificazione, riducendo dati personali, dettagli sfruttabili e riproduzione di contenuti nocivi.^[1]

5. Identità e mandato dell'ONPAC-OLITEC

Un centro civile di monitoraggio, ricerca e resilienza cognitiva

L'ONPAC-OLITEC sarà un'unità permanente interna alla Fondazione Olivetti Tecnologia e Ricerca, senza finalità di lucro, dotata di autonomia scientifica, metodologica ed editoriale nei limiti della responsabilità giuridica, amministrativa e finanziaria della Fondazione. Il suo valore non dipenderà da poteri coercitivi, ma dalla qualità delle evidenze, dalla trasparenza del metodo e dalla capacità di costruire cooperazione.

Missione

La missione consiste nell'osservare la proliferazione delle capacità tecniche e organizzative idonee a influenzare o degradare processi cognitivi individuali e collettivi; documentare gli impieghi rilevati nel contesto italiano; valutare rischio, danno, vulnerabilità, resilienza e contromisure; produrre rapporti pubblici e raccomandazioni applicabili. L'analisi sarà centrata sui comportamenti e sulle modalità operative, non sulle opinioni politiche, culturali, religiose o scientifiche espresse nei contenuti.^[1]

Obiettivi strategici 2027–2029

- Costruire una definizione operativa, prudente e verificabile delle armi cognitive e delle capacità dual use.
- Rilevare tempestivamente segnali di manipolazione coordinata e impieghi ad alto impatto nello spazio informativo italiano.
- Sviluppare una base dati comparabile nel tempo, distinguendo l'aumento del fenomeno dall'aumento della capacità di osservazione.
- Misurare vulnerabilità, esposizione, persistenza, danno e capacità di risposta senza creare profili ideologici di persone o comunità.
- Favorire cooperazione tra ricerca, autorità, piattaforme, media, fact-checker, imprese e società civile.
- Rafforzare alfabetizzazione mediatica, cognitiva e tecnologica attraverso formazione, protocolli ed esercitazioni difensive.
- Produrre White Paper autorevoli, replicabili, accessibili e utili alle decisioni pubbliche e private.

Campo di osservazione

Famiglia	Capacità osservate
Produzione e falsificazione	Testi sintetici, immagini, audio, video, documenti, cloni vocali e impersonificazione.
Distribuzione e amplificazione	Bot, account coordinati, brigading, cross-posting, pubblicità, SEO e manipolazione dei recommender.
Targeting e profilazione	Micro-targeting, segmentazione, inferenza emotiva, look-alike e sfruttamento di vulnerabilità.
Interfacce e attenzione	Dark pattern, nudging occulto, sovraccarico, ricompense variabili e frizioni selettive.
Immersivo e incarnato	VR/AR, avatar, presenza sociale, manipolazione sensoriale e spaziale.
Neurocognitivo e biometrico	Eye tracking, voce, volto, fisiologia, BCI e inferenze comportamentali.
Agenti autonomi	Chatbot, companion, agenti sociali, sistemi multiagente e personalizzazione continua.
Cyber-cognitivo	Account compromessi, leak, siti clonati, data poisoning e contaminazione delle fonti.
Organizzativo-decisionale	Dashboard, metriche, ranking, consenso sintetico e modelli predittivi usati nelle decisioni.

Tre garanzie non negoziabili

Garanzia	Applicazione
Neutralità	Si analizzano inganno, coordinamento, targeting, automazione, scala ed effetti. Dissenso, critica, satira, giornalismo e comunicazione politica lecita non sono minacce in quanto tali.
Prova	Ogni affermazione pubblica è collegata a un fascicolo, a fonti tracciate, a un livello di confidenza e a una revisione indipendente. Un rilevatore automatico isolato non basta.
Proporzionalità	La pubblicazione deve arrecare meno danno del fenomeno documentato. Si minimizzano dati personali, esposizione dei vulnerabili, dettagli sfruttabili e amplificazione.

Attività escluse

L'Osservatorio non svolgerà sorveglianza generalizzata di persone, intercettazione di comunicazioni private, accesso abusivo, acquisizione di credenziali, infiltrazione non autorizzata, acquisto di dati illeciti, riconoscimento biometrico di massa, diagnosi psicologica o profilazione ideologica individuale. Non condurrà operazioni di influenza contro persone o popolazioni reali. Eventuali test di red team o simulazioni saranno ammessi soltanto in sandbox, con scenari sintetici o partecipanti informati, approvazione etica, minimizzazione dei dati, kill switch e divieto di diffusione involontaria.^[1]

Nessun automatismo

Propaganda, marketing, comunicazione politica, satira, linea editoriale, moderazione dei contenuti, sistemi di raccomandazione, uso dell'IA generativa e ambienti immersivi non saranno classificati automaticamente come armi cognitive. L'inquadramento richiederà indicatori contestuali, probatori e di impatto ulteriori.^[1]

6. Governance e profili di coinvolgimento

Come saranno distribuite responsabilità, revisione e controllo

La governance è progettata per evitare concentrazioni di potere e separare indirizzo amministrativo, supervisione scientifica ed etica, valutazione dei casi, gestione operativa e comunicazione. Nessun singolo esperto e nessun algoritmo dovranno poter determinare da soli l'apertura, l'attribuzione o la pubblicazione di un caso sensibile.

Architettura di governo

Componente	Funzione
Consiglio di amministrazione della Fondazione	Approva programma, piano annuale, budget e rendiconto; nomina gli organi; assicura risorse, coperture, consulenza legale e presidi di sicurezza; riceve il White Paper senza modificarne le conclusioni scientifiche.
Comitato Scientifico Tecnico Etico	Approva metodologia, codice etico, priorità e protocolli; valuta rischi per diritti e libertà; esprime parere obbligatorio su White Paper e studi sensibili.
Comitato Tecnico di Valutazione	Costituisce il gate di qualità dei fascicoli pubblicabili; verifica prova, confidenza, proporzionalità, replica e coerenza metodologica con revisori indipendenti.
Direttore dell'Osservatorio	Guida strategia e attività, propone il piano, assegna i fascicoli, garantisce tempi e procedure, cura relazioni istituzionali e firma le pubblicazioni.
Unità Operativa	Raccoglie segnali, conduce analisi, forensics, valutazione d'impatto, case management, sicurezza dei dati, legale/privacy e comunicazione scientifica.
Rete consultiva e territoriale	Università, centri di ricerca, professionisti, media, fact-checker, organizzazioni civiche e delegati territoriali forniscono segnali, competenze e revisione senza potere decisionale sui casi.

Profili professionali ricercati

Area	Contributo atteso
IA e data science	Modelli generativi e agentici, analisi dati, valutazione degli strumenti, limiti e bias.
Cybersecurity e OSINT	Raccolta lecita, analisi di infrastrutture e reti, provenienza, incident response e responsible disclosure.
Media forensics	Verifica di immagini, audio, video, documenti, metadati e catena di custodia.
Psicologia cognitiva e neuroscienze	Processi decisionali, vulnerabilità, effetti, strumenti di impatto ed etica dei test.
Sociologia e scienza politica	Dinamiche collettive, coesione, processi democratici, campagne e contesto.
Diritto e protezione dei dati	Basi giuridiche, DPIA, reputazione, segreto, diritto di replica, whistleblowing e referral.
Media e comunicazione	Ecosistema informativo, giornalismo, fact-checking, comunicazione di crisi e divulgazione responsabile.
Realtà immersiva e HCI	Avatar, ambienti VR/AR, interazioni multisensoriali, design persuasivo e dati biometrici.
Difesa, sicurezza e decisione	Scenari strategici, protezione delle decisioni, formazione e raccordo con gli interlocutori istituzionali.
Educazione e alfabetizzazione	Progettazione di strumenti accessibili per scuole, famiglie, cittadini, imprese e amministrazioni.

Forme di coinvolgimento possibili

Forma	Contributo	Impegno caratteristico
Componente del Comitato Scientifico Tecnico Etico	Supervisione, metodo, etica, priorità, White Paper	Mandato pluriennale; riunioni programmate e pareri su studi sensibili
Componente del Comitato Tecnico di Valutazione	Revisione indipendente di fascicoli e pubblicazioni	Disponibilità per revisioni, astensione nei conflitti, controllo di prova e proporzionalità
Ruolo direttivo o operativo	Gestione, monitoraggio, analisi, dati, forensics, legale, sicurezza o redazione	Impegno continuativo, formazione, responsabilità su procedure e livelli di servizio
Revisore esterno	Peer review di rapporti o studi specifici	Intervento circoscritto, dichiarazione di interessi, rispetto di embargo e riservatezza
Partner della rete consultiva	Segnali, dati, competenze, ricerca, formazione o territorialità	Accordo che preservi indipendenza, finalità, privacy e assenza di veto sui risultati
Delegato territoriale	Ascolto, formazione, segnalazione e raccordo locale	Nessun potere investigativo o comunicazione pubblica non autorizzata; formazione obbligatoria

Indipendenza, conflitti e finanziamenti

Ogni incaricato dovrà dichiarare interessi economici, professionali, politici, accademici e associativi rilevanti. Il conflitto effettivo comporterà astensione; quello potenziale sarà valutato e registrato. Saranno vietati finanziamenti destinati a ottenere o impedire l'apertura di un caso, influenzarne l'esito o anticiparne la pubblicazione. I contributi provenienti da soggetti industriali interessati dal perimetro saranno ammissibili soltanto con firewall, trasparenza e assenza di vincoli sui risultati. La sostenibilità economica non dovrà trasformarsi in dipendenza scientifica.^[1]

Il criterio di qualità della governance

La pluralità disciplinare non basta se le persone non accettano la revisione reciproca. Il modello richiede che chi raccoglie le prove non sia l'unico a valutarle, che le attribuzioni sensibili siano sottoposte a controllo legale ed etico e che le decisioni rimangano tracciate in un audit trail.

7. Metodo operativo

Dal segnale alla pubblicazione: come si evita che il monitoraggio diventi sospetto o accusa

Il valore dell'Osservatorio dipenderà dalla capacità di trasformare segnali eterogenei in valutazioni riproducibili, mantenendo separati rischio, prova, attribuzione e giudizio giuridico. Il metodo è costruito per ridurre falsi positivi, politicizzazione e danno reputazionale e per permettere la correzione pubblica degli errori.

Architettura informativa

Archivio	Funzione
Repertorio dei sistemi e delle capacità	Tecnologie, metodologie e servizi rilevanti; versioni, accessibilità, costo, scalabilità, targeting, occultamento e salvaguardie.
Registro dei segnali, incidenti e campagne	Segnalazioni, eventi, asset, cronologie, tecniche, livelli di rischio, confidenza e stato osservativo.
Quadro delle vulnerabilità e della resilienza	Settori, territori, processi esposti, capacità di risposta, formazione, protocolli e contromisure.

Flusso di lavorazione

Fase	Attività	Termine ordinario
1. Ricezione	Protocollo, identificativo, controllo malware, livello di riservatezza	Automatico o entro 1 giorno lavorativo

Fase	Attività	Termine ordinario
2. Triage	Collegamento con l'Italia, perimetro cognitivo, urgenza, liceità e duplicati	Entro 3 giorni; in giornata se urgente
3. Valutazione preliminare	Fonti, ipotesi alternative, primo punteggio e piano di lavoro	Entro 10 giorni
4. Analisi	Raccolta, forensics, rete, impatto, cronologia e contatti	30 giorni; proroga motivata fino a 60
5. Doppia revisione	Secondo analista, controllo legale/etico e riconciliazione dello score	5-10 giorni
6. Replica	Invio di una sintesi ai soggetti nominati e verifica della risposta	10 giorni; 3 nei casi urgenti
7. Decisione	Pubblicazione, nota riservata, referral o archiviazione	Entro 5 giorni dalla revisione
8. Follow-up	Aggiornamento, effetti, correzioni e chiusura	Trimestrale per casi aperti

Standard probatori

Ogni elemento sarà valutato per affidabilità della fonte, integrità, contemporaneità, indipendenza, corroborazione e riproducibilità. I contenuti digitali saranno preservati, ove lecito, con data e ora, origine, hash, screenshot o copia, metadati e indicazione dello strumento di acquisizione. Per immagini, audio e video i detector automatici saranno considerati indizi, non prove decisive: l'analisi combinerà provenienza, metadati, confronto con originali, reverse search, esame forense, conferma del soggetto impersonato, contesto e comportamento della rete di diffusione.^[1]

Rischio e confidenza: due misure diverse

Il punteggio di rischio descrive la gravità potenziale o osservata del fenomeno; il livello di confidenza descrive quanto sono solide le prove. Un caso può essere ad alto rischio ma avere confidenza limitata: in questa situazione richiede attenzione e verifica, non un'attribuzione pubblica. Separare le due dimensioni impedisce che l'urgenza sostituisca la prova e che una prova tecnica robusta faccia apparire grave un caso in realtà circoscritto.

Dimensione	Peso max	Criterio
Gravità del danno	25	Danno fisico, psicologico, economico, reputazionale, democratico o di sicurezza
Portata/esposizione	15	Numero e ampiezza dei destinatari, inclusa crescita rapida
Vulnerabilità/criticità	15	Minori, fragili, servizi essenziali, elezioni, salute, emergenze
Intensità manipolativa	15	Inganno, occultamento, coercizione, impersonificazione, compromissione dell'autonomia
Coordinamento e automazione	10	Reti, agenti, bot, sincronizzazione, adattamento
Persistenza e multiplatforma	10	Durata, ripetizione, resistenza alle correzioni, contaminazione di archivi
Sensibilità strategica/temporale	10	Prossimità a voto, crisi, conflitto, mercato, emergenza o decisione critica

Punteggio	Fascia	Azione minima
0-19	Routine	Registrazione e monitoraggio; nessuna pubblicazione di caso
20-39	Rilevante	Pre-fascicolo, raccolta aggiuntiva e verifica di trend
40-59	Significativo	Fascicolo completo e revisione senior
60-79	Alto	Valutazione urgente, contatto con soggetti colpiti e possibile avviso
80-100	Critico	Protocollo di crisi, segnalazioni istituzionali e comunicazione prioritaria se utile

Livello	Descrizione	Regola editoriale
C0 - Insufficiente	Segnale singolo, contraddittorio o non verificabile; output automatico isolato	Solo uso interno o dato aggregato; nessuna attribuzione
C1 - Limitata	Indicatori coerenti ma fonti incomplete o dipendenti; alternative rilevanti	Pubblicazione solo se necessaria, anonimizzata e con forte cautela

Livello	Descrizione	Regola editoriale
C2 - Moderata	Più elementi indipendenti o prova tecnica robusta; incertezze circoscritte	Caso pubblicabile con limiti e repliche evidenziate
C3 - Alta	Linee probatorie indipendenti convergenti, provenienza e revisione, nessuna contraddizione materiale	Possibile attribuzione nominativa, previa verifica legale e diritto di replica

Protocollo urgente e referral

Il protocollo urgente potrà attivarsi anche indipendentemente dal punteggio complessivo quando vi siano pericolo imminente per persone, interferenza con il voto o con informazioni di servizio elettorale, impersonificazione di autorità di emergenza, rischio per minori, compromissione di infrastrutture o fonti pubbliche, panico, frode estesa o grave danno economico. L'Osservatorio non sostituirà i soccorsi o le autorità: predisporrà una scheda rapida con fatti, incertezze, rischio e destinatari e valuterà il trasferimento secondo canali formalizzati.^[1]

Gate di pubblicazione

Controllo	Criterio di superamento
Perimetro	Collegamento sostanziale con l'Italia e finalità cognitiva definiti
Prova	Fonti tracciate, materiali preservati, ipotesi alternative considerate
Rischio/confidenza	Punteggi separati, doppia valutazione e divergenze risolte
Attribuzione	Asset, operatore, sponsor e beneficiario distinti; soglia di naming rispettata
Dati personali	Base giuridica, minimizzazione e anonimizzazione verificate
Diritto di replica	Soggetto contattato o deroga urgente motivata
Danno informativo	Ridotta riproduzione di contenuti nocivi e dettagli sfruttabili
Revisione	Pareri tecnico, legale/etico ed editoriale acquisiti
Linguaggio	Fatti, inferenze, ipotesi e limiti esplicitamente distinti
Follow-up	Responsabile, data di riesame e canale di correzione definiti

Indicatore vietato

Il numero di persone, aziende, partiti o Stati "segnalati" non sarà un indicatore di performance. Un incentivo fondato sul volume dei casi aumenterebbe falsi positivi, politicizzazione e danno reputazionale. La qualità sarà misurata attraverso tempi, revisione, correzioni, sicurezza, coerenza e trasparenza.^[1]

8. Programma dei White Paper

Una base probatoria comune, tre versioni per lettori diversi

Lo scopo pubblico principale dell'ONPAC-OLITEC sarà redigere uno o più White Paper capaci di trasformare l'osservazione in conoscenza utilizzabile. Il rapporto annuale costituirà il riferimento nazionale; a esso potranno affiancarsi documenti tematici quando un settore, una tecnologia o un evento richiedano un approfondimento specifico. Tutte le pubblicazioni dovranno essere comprensibili anche a chi non possiede un background informatico o militare, separando il corpo principale dagli allegati tecnici.

Il White Paper nazionale annuale

Il rapporto ordinario avrà il titolo "Armi cognitive in Italia: sistemi, impieghi, incidenti e resilienza - Rapporto [anno]". Coprirà il periodo 1° gennaio-31 dicembre e sarà pubblicato, dopo un anno pieno di osservazione, entro il 30 aprile successivo. Comprenderà governance e finanziamenti, metodologia e limiti, capacità e livelli di proliferazione, usi legittimi e duali, incidenti e campagne, analisi settoriale e territoriale, effetti, vulnerabilità, risposte, raccomandazioni, dati aggregati e correzioni. Ogni edizione sarà sottoposta ad almeno tre revisioni esterne, controllo legale ed etico e verifica del diritto di replica.^[1]

Rapporto zero e White Paper tematici

Durante il primo anno sarà prodotto un "Rapporto zero", dedicato soprattutto a metodologia, copertura, limiti, qualità dei dati e risultati iniziali. Non dovrà simulare una rappresentatività nazionale non ancora raggiunta. Successivamente potranno essere pubblicati White Paper tematici su periodi elettorali, deepfake e impersonificazione, minori, agenti autonomi, ambienti immersivi e neurotecnologie, salute ed emergenze, cyber-cognitivo, sistemi decisionali o settori economici specifici. L'apertura di un filone tematico dipenderà dal piano annuale, dalle evidenze e dalle risorse, non dalla pressione mediatica.

Le tre versioni per comunità di lettori

VERSIONE 1 ISTITUZIONALE E DI POLICY	VERSIONE 2 DIFESA E SICUREZZA	VERSIONE 3 CIVILE E DIVULGATIVA
Destinatari: Governo, Parlamento, amministrazioni, autorità, servizi essenziali, decisori pubblici.	Destinatari: Forze Armate, istituti di formazione della difesa, strutture di sicurezza e protezione decisionale.	Destinatari: cittadini, scuole, famiglie, media, associazioni, professionisti e PMI.
Focus: quadro nazionale, lacune di coordinamento, impatti normativi, priorità, raccomandazioni, indicatori e opzioni di policy.	Focus: scenari, indicatori, resilienza della decisione, esercitazioni difensive, cooperazione civile-militare. Nessun dettaglio offensivo o informazione classificata.	Focus: linguaggio chiaro, esempi, riconoscimento dei segnali, protezione quotidiana, alfabetizzazione, procedure di segnalazione e strumenti pratici.

Figura 5 - Le tre versioni condividono dati, metodo, livelli di prova e conclusioni; cambiano profondità, lessico e strumenti di utilizzo.

Una sola evidenza, nessuna verità parallela

La differenziazione per lettore non dovrà produrre messaggi incompatibili. Le tre versioni useranno la stessa base dati, gli stessi fascicoli, la stessa tassonomia, gli stessi livelli di confidenza e gli stessi limiti. La versione istituzionale approfondirà scelte e coordinamento; quella per difesa e sicurezza tradurrà le evidenze in scenari di protezione e formazione; quella civile eliminerà il gergo e offrirà strumenti pratici. Le informazioni sensibili o i dettagli che faciliterebbero l'abuso saranno esclusi o ridotti in tutte le versioni.

Destinazione e distribuzione

Versione	Destinatari	Modalità di diffusione
Istituzionale e di policy	Presidenza del Consiglio, ministeri competenti, commissioni parlamentari, autorità indipendenti, amministrazioni centrali e territoriali, soggetti responsabili di servizi essenziali	Trasmissione formale, briefing, consultazioni e raccomandazioni non vincolanti
Difesa e sicurezza	Vertici e strutture delle Forze Armate, istituti di formazione, organismi di sicurezza e partner istituzionali secondo competenza	Briefing, moduli formativi, scenari ed esercitazioni difensive; eventuali circuiti controllati per materiale non pubblico
Civile e divulgativa	Cittadini, scuole, università, famiglie, media, associazioni, ordini professionali, imprese e PMI	Pubblicazione aperta, sintesi accessibili, infografiche, webinar, toolkit e materiali educativi

Calendario editoriale ordinario

Scadenza	Attività
Entro 31 gennaio	Pubblicazione di metodologia, perimetro, priorità e principali fonti
Trimestralmente	Calibrazione analisti, revisione watchlist, controllo bias e registro delle modifiche
30 settembre	Piano editoriale preliminare, selezione dei casi e nomina dei revisori esterni
31 dicembre	Chiusura del periodo di osservazione
Gennaio-febbraio	Pulizia dati, analisi, redazione e verifiche metodologiche e legali
Marzo	Peer review, repliche, correzioni e approvazione degli organi
Entro 30 aprile	Pubblicazione, presentazione e dataset aggregato
Entro 30 giugno	Risposte alle osservazioni principali e nota di aggiornamento, se necessaria

Regole editoriali

- I conteggi osservati non saranno presentati come prevalenza nazionale se la raccolta non è rappresentativa.
- Ogni percentuale indicherà denominatore, periodo, fonte e criterio di inclusione.
- La crescita dei casi sarà separata dalla crescita delle fonti, del personale e della capacità di rilevazione.
- Stime e scenari saranno accompagnati da metodo, incertezza e sensibilità alle ipotesi.
- Casi non corroborati, smentite, correzioni e falsi positivi saranno rendicontati.
- Non saranno pubblicate graduatorie ideologiche, liste nere o punteggi di affidabilità personale.
- Ogni edizione manterrà un archivio di versione e un errata corrige permanente.

Obiettivo finale dei White Paper

Creare un linguaggio comune tra istituzioni, difesa, ricerca e società; offrire una base di evidenze verificabili; indicare vulnerabilità e contromisure proporzionate; rendere i cittadini più capaci di riconoscere la manipolazione senza indurre paura o sfiducia generalizzata.

9. Avvio, roadmap e criteri di maturità

Dall'inaugurazione di gennaio 2027 a una capacità nazionale verificabile

La costruzione dell'Osservatorio sarà graduale. Un lancio pubblico non equivale automaticamente a una capacità operativa completa: dichiarare copertura nazionale o servizio continuativo prima di disporre di persone, processi e infrastrutture adeguati comprometterebbe la credibilità. Il primo anno sarà quindi una fase di fondazione, pilotaggio e validazione.

Roadmap dei primi dodici mesi

Mese	Azioni	Deliverable
0-1	Deliberazione, nomina del Direttore, costituzione degli organi, budget e responsabili	Atto istitutivo e organigramma
1-2	Registro trattamenti, valutazione privacy preliminare, policy sicurezza, conflitti e canali di segnalazione	Pacchetto compliance
2-3	Tassonomia, schema dati, procedure di prova, scoring e manuale analisti	Metodologia v0.9
3-4	Infrastruttura, evidence vault, case management, sito trasparenza e logging	Ambiente di pilotaggio
4-5	Formazione iniziale, esercizi sintetici, calibrazione e test di sicurezza	Analisti abilitati e report test
5-7	Pilota su due settori e fonti definite, senza pretesa di copertura nazionale	Bollettino pilota riservato
7-8	Audit metodologico, privacy e sicurezza; correzione dei processi	Audit e metodologia v1.0
8-9	Lancio pubblico operativo, portale segnalazioni e prime partnership	Sito e protocollo partner
9-11	Estensione graduale, primo bollettino pubblico e peer review dei fascicoli	Bollettino semestrale
12	Valutazione, rendiconto, Rapporto zero e piano del secondo anno	Rapporto zero e piano annuale

Criteri di go-live

- Direttore, Comitato Scientifico Tecnico Etico e Comitato Tecnico di Valutazione formalmente operativi.
- Metodologia pubblica, tassonomia, scoring, procedure di replica e correzione approvati.
- Registro dei trattamenti, valutazioni privacy e canale del responsabile protezione dati attivi.
- Infrastruttura testata, backup verificato, evidence vault e controllo accessi funzionanti.
- Almeno due esercitazioni su casi sintetici concluse senza violazioni critiche.
- Accordo inter-valutatore misurato e piano di calibrazione adottato.
- Registro dei finanziatori e dichiarazioni di conflitto disponibili.
- Protocollo di crisi e matrice dei contatti istituzionali verificati.
- Policy editoriale, diritto di replica e pagina delle correzioni pubblicati.
- Piano annuale e calendario del White Paper approvati.

Modelli di risorse

Modello	Copertura	Limiti
Pilota	5-6 FTE; fonti selezionate; due settori; orario lavorativo	Nessuna pretesa di rappresentatività nazionale; alert limitati agli ambiti definiti
Ordinario	10-12 FTE; copertura multisettoriale; rete di partner; White Paper completo	Reperibilità limitata; analisi profonda selettiva
Rafforzato	18+ FTE; turnazione; lingue e aree specialistiche; incident response continuativo	Richiede budget pluriennale, infrastruttura sicura e governance più articolata

Il modello pilota è sufficiente per validare procedure e produrre un Rapporto zero, ma non può sostenere una promessa di copertura nazionale piena. Il modello ordinario consente osservazione multisettoriale e produzione del White Paper; un servizio 24/7 richiede turnazione dedicata, reperibilità, sicurezza e risorse ulteriori e non dovrà essere dichiarato finché non sia effettivamente attivo. Questa gradualità protegge tanto l'efficacia quanto la reputazione dell'iniziativa. ^[1]

Valutazione indipendente

Entro dodici mesi è previsto un audit indipendente su metodo, dati, sicurezza, conflitti e qualità editoriale. Entro il ventiquattresimo mese una valutazione esterna dovrà esaminare utilità pubblica, neutralità, protezione dei dati, sostenibilità e impatto delle raccomandazioni. Potrà proporre revisioni del perimetro, riduzione di attività invasive, estensione delle competenze o sospensione di procedure non validate. L'Osservatorio dovrà dimostrare di saper apprendere e, quando necessario, limitarsi. ^[1]

Gennaio 2027: che cosa si inaugura

L'evento di gennaio dovrà presentare missione, governance in costituzione, metodo, piano di avvio e rete di interlocuzione. La comunicazione pubblica dovrà distinguere chiaramente l'inaugurazione istituzionale dalla piena capacità operativa, che sarà raggiunta per fasi e documentata attraverso i criteri di maturità.

10. Impegno richiesto ai candidati

Competenze, comportamento e responsabilità prima dell'adesione

La partecipazione all'ONPAC-OLITEC richiede più della competenza specialistica. Il candidato deve essere disponibile a operare in un ambiente interdisciplinare, sottoporsi a revisione, gestire incertezza e informazioni sensibili e tradurre concetti complessi in conclusioni prudenti. Una reputazione elevata non sostituisce il rispetto delle procedure; l'autorevolezza dell'Osservatorio nascerà dalla disciplina collettiva.

Requisiti trasversali

Requisito	Comportamento atteso
Indipendenza	Capacità di separare analisi, preferenze personali, interessi professionali e appartenenze; disponibilità all'astensione.
Rigore probatorio	Distinguere fatti, inferenze, ipotesi e scenari; documentare fonti, limiti e spiegazioni alternative.
Prudenza comunicativa	Evitare sensazionalismo, anticipazioni, accuse e semplificazioni che amplifichino il danno.
Riservatezza	Proteggere fonti, dati, casi, materiali non pubblici, credenziali e informazioni ricevute dai partner.
Capacità interdisciplinare	Comprendere il contributo degli altri domini e accettare che una conclusione tecnica possa richiedere limiti legali, etici o sociali.
Responsabilità correttiva	Segnalare errori, cooperare al riesame e accettare correzioni pubbliche e cronologia delle versioni.
Orientamento civile e difensivo	Non utilizzare attività, dati o strumenti dell'Osservatorio per influenza offensiva, sorveglianza impropria o vantaggio di parte.
Accessibilità	Saper comunicare a decisori e cittadini non specialisti senza perdere precisione.

Obblighi prevedibili

- Presentazione di curriculum e dichiarazione iniziale e annuale di interessi rilevanti.
- Sottoscrizione degli impegni di riservatezza, sicurezza e uso autorizzato dei sistemi.
- Partecipazione alla formazione metodologica, alle esercitazioni e alle calibrazioni periodiche.
- Astensione da casi nei quali esista conflitto effettivo o rischio ragionevole di parzialità.
- Uso esclusivo di canali e strumenti approvati per materiali e comunicazioni dell'Osservatorio.
- Rispetto delle regole di comunicazione pubblica: nessuna dichiarazione su casi o fonti senza autorizzazione.
- Disponibilità a fornire motivazioni scritte, revisioni e osservazioni secondo tempi ragionevoli.
- Collaborazione al diritto di replica, alla gestione dei reclami e alla correzione degli errori.

Domande di autovalutazione

1

Domanda

Sono disposto a modificare una conclusione quando emergono prove migliori, anche se la prima ipotesi era plausibile?

2

Domanda

Riesco a lavorare con incertezza senza trasformarla in sospetto o attribuzione?

3

Domanda

Posso mantenere riservatezza anche quando un caso genera attenzione mediatica o interesse professionale?

4

Domanda

Sono disponibile a dichiarare interessi e ad astenermi senza interpretare l'astensione come perdita di prestigio?

5

Domanda

So spiegare il mio contributo a colleghi di discipline diverse e a lettori non specialisti?

6

Domanda

Accetto che la pubblicazione debba talvolta essere rinviata o esclusa per prova insufficiente o rischio di danno?

7

Domanda

Posso dedicare tempo continuativo, non soltanto intervenire in occasioni pubbliche?

Percorso di coinvolgimento

Fase	Contenuto
1. Manifestazione di interesse	Disponibilità, area di competenza, forma di coinvolgimento preferita e tempo indicativo.
2. Valutazione preliminare	Esame del profilo, compatibilità con il fabbisogno e verifica iniziale di indipendenza.
3. Colloquio tecnico e valoriale	Discussione su metodo, responsabilità, casi ipotetici e capacità interdisciplinare.
4. Dichiarazioni e verifiche	Interessi, riservatezza, requisiti, eventuali incompatibilità e riferimenti professionali.
5. Atto formale	Nomina, incarico, accordo o adesione alla rete secondo la posizione; definizione di durata e responsabilità.
6. Formazione e abilitazione	Induzione, procedure, sicurezza, prova, privacy, comunicazione e simulazioni sintetiche.
7. Valutazione periodica	Contributo, qualità, conflitti, formazione e rispetto delle regole; rinnovo non automatico.

Natura dell'adesione

Il dossier non costituisce invito irrevocabile né promessa di nomina. La composizione finale dovrà rispettare equilibrio disciplinare, indipendenza, sostenibilità e capacità effettiva di lavoro. Anche candidature di altissimo profilo potranno essere orientate verso ruoli consultivi o di revisione più adatti alla disponibilità e all'assenza di conflitti.

Appendice A – Tassonomia sintetica delle capacità cognitive

Famiglie osservate e indicatori di possibile trasformazione offensiva

Famiglia	Capacità	Indicatori di weaponization
A. Produzione e falsificazione	Testi, immagini, audio, video, documenti, cloni vocali, impersonificazione	Falsa attribuzione, occultamento, adattamento rapido, volume, impiego in decisioni
B. Distribuzione e amplificazione	Bot, account coordinati, cross-posting, ad network, SEO e recommender gaming	Sincronizzazione, inautenticità, crescita non organica, elusione e migrazione
C. Targeting e profilazione	Micro-targeting, segmentazione, inferenza emotiva, look-alike e personalizzazione	Dati sensibili, consenso carente, messaggi incompatibili, sfruttamento di fragilità
D. Interfacce e attenzione	Dark pattern, nudging occulto, overload, ricompense variabili, frizione selettiva	Compromissione della scelta informata, dipendenza, impossibilità pratica di rifiuto
E. Immersivo e incarnato	VR/AR, avatar, simulazioni, presenza sociale, manipolazione sensoriale e spaziale	Impersonificazione di autorità, stimoli invisibili, biometria, assenza di uscita
F. Neurocognitivo e biometrico	BCI, eye tracking, voce, volto, fisiologia e inferenze comportamentali	Uso non consensuale, targeting di stati mentali, adattamento persuasivo
G. Agenti autonomi	Chatbot, companion, agenti sociali, sistemi multiagente, personalizzazione continua	Autonomia, memoria del bersaglio, coordinamento, escalation e persuasione adattiva
H. Cyber-cognitivo	Account compromessi, leak, siti clonati, data poisoning e knowledge base	Autenticità rubata, narrativa preparata, timing strategico, danno alla fiducia
I. Organizzativo-decisionale	Dashboard, sistemi di supporto, metriche, ranking, consenso sintetico e modelli predittivi	Dati manipolati, opacità, autorità indebita, impatto su decisioni collettive

La presenza di un indicatore non prova da sola l'esistenza di un'arma cognitiva. Il profilo di proliferazione descrive accessibilità, costo, competenze richieste, scalabilità, targeting, occultamento, autonomia, multimodalità, persistenza e contromisure. La valutazione offensiva richiede sempre il contesto d'uso, la finalità, il danno e la solidità delle prove. ^[1]

Appendice B – Stati osservativi e linguaggio pubblico

Come evitare che un segnale venga presentato come fatto accertato

Stato	Significato
L0 – Capacità	Sistema o tecnica dual use, senza evidenza di impiego dannoso nel caso considerato
L1 – Indicatore	Segnale di rischio o proliferazione da osservare
L2 – Incidente sospetto	Possibile uso manipolativo non ancora corroborato
L3 – Uso corroborato	Impiego manipolativo verificato con confidenza almeno moderata
L4 – Campagna	Attività collegate, coordinate o persistenti con obiettivo comune
L5 – Attacco cognitivo	Campagna o evento ad alto impatto, con prova forte e rilevanza strategica; attribuzione separata

Le pubblicazioni utilizzeranno formule standardizzate come “segnale”, “incidente sospetto”, “uso corroborato”, “campagna” o “attacco”, accompagnate da rischio e confidenza. I comunicati distingueranno fatti, inferenze, ipotesi e raccomandazioni. Titoli sensazionalistici, ripetizione di falsità e immagini nocive non necessarie saranno evitati. ^[1]

Appendice C – Glossario essenziale

Definizioni in linguaggio accessibile

Termine	Spiegazione
Agente autonomo	Sistema di IA capace di pianificare o svolgere più azioni, adattandosi ai risultati con un grado variabile di autonomia.
Astroturfing	Simulazione artificiale di un sostegno o di una protesta spontanea attraverso account, gruppi o contenuti coordinati.
Bot	Account o programma che esegue automaticamente azioni, come pubblicare, rispondere o amplificare contenuti.
Confidenza	Misura della solidità delle prove, distinta dalla gravità del rischio.
Dark pattern	Interfaccia progettata per spingere l'utente verso una scelta, rendendo meno visibili o più difficili le alternative.
Data poisoning	Inserimento o alterazione di dati per compromettere un sistema di analisi, ricerca o intelligenza artificiale.
Deepfake	Contenuto audio, video o immagine generato o manipolato per rappresentare in modo realistico persone o eventi non autentici.
FIMI	Manipolazione e interferenza informativa straniera: comportamento intenzionale e coordinato che può danneggiare valori o processi politici.
Impersonificazione	Uso non autorizzato di identità, voce, volto, ruolo o segni di un soggetto per indurre altri in errore.
Micro-targeting	Invio di messaggi differenziati a gruppi molto specifici sulla base di dati e caratteristiche inferite.
OSINT	Raccolta e analisi di informazioni ottenute legalmente da fonti aperte e accessibili.
Payload informativo	Contenuto o messaggio veicolato attraverso un accesso o un incidente cyber per produrre un effetto cognitivo.
Provenienza	Informazioni che permettono di ricostruire origine, modifiche e percorso di un contenuto.
Resilienza cognitiva	Capacità di riconoscere manipolazioni, mantenere qualità decisionale, correggere errori e recuperare fiducia.
Weaponization	Trasformazione funzionale di una capacità legittima o dual use in uno strumento offensivo attraverso modalità concrete di impiego.

Fonti essenziali

Documenti istituzionali e scientifici utilizzati per lo scenario e la progettazione

- [1] Fondazione Olivetti Tecnologia e Ricerca – OLITEC, Osservatorio Nazionale sulla Proliferazione delle Armi Cognitive: Programma istitutivo, regolamento e manuale operativo, bozza v1.1, luglio 2026.
- [2] NATO Defense College, The Human Mind as a Battlespace: Insights from the Conference of Commandants 2026, 24 giugno 2026. [Fonte ufficiale](#)
- [3] NATO Defense College, War is a mind game: countering weaponised information, NDC Outlook 2026-01, 23 gennaio 2026. [Fonte ufficiale](#)
- [4] European External Action Service / EUvsDisinfo, 4th EEAS Annual Report on Foreign Information Manipulation and Interference Threats, 12 marzo 2026. [Fonte ufficiale](#)
- [5] OECD, Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity, 4 marzo 2024. [Fonte ufficiale](#)
- [6] ENISA, Threat Landscape 2025 – EU consistently targeted by diverse yet convergent threat groups, 2025. [Fonte ufficiale](#)
- [7] Autorità per le Garanzie nelle Comunicazioni, Rapporto Intelligenza Artificiale 2026, 17 giugno 2026. [Fonte ufficiale](#)
- [8] Autorità per le Garanzie nelle Comunicazioni, Osservatorio annuale sul sistema dell'informazione – II edizione, 2026. [Fonte ufficiale](#)
- [9] ISTAT, Cittadini e ICT – Anno 2025, pubblicato nel 2026; e Infografiche – Rapporto annuale 2026. [Fonte ufficiale](#)
- [10] Commissione europea, Relazione per paese sul decennio digitale 2026 dell'Italia, 2026. [Fonte ufficiale](#)
- [11] Garante per la protezione dei dati personali, Relazione 2025 e materiali istituzionali su deepfake, minori e intelligenza artificiale, 2026. [Fonte ufficiale](#)
- [12] Legge 23 settembre 2025, n. 132, Disposizioni e deleghe al Governo in materia di intelligenza artificiale. [Fonte ufficiale](#)
- [13] Unione europea, Regolamento (UE) 2022/2065 – Digital Services Act; materiali sul coordinamento nazionale e relazione AGCOM 2025. [Fonte ufficiale](#)
- [14] Unione europea, Regolamento (UE) 2024/900 sulla trasparenza e il targeting della pubblicità politica. [Fonte ufficiale](#)

Le fonti online sono state consultate il 19 luglio 2026. I dati quantitativi citati nel dossier devono essere aggiornati prima di ogni futura edizione o trasmissione istituzionale. Le informazioni tratte dal rapporto EEAS rappresentano il campione di attività rilevate e analizzate dall'istituzione e non una stima esaustiva della diffusione globale.

Conclusione

Un invito a costruire un presidio credibile, utile e responsabile

L'ONPAC-OLITEC nasce dall'idea che la libertà di pensiero non si protegga scegliendo al posto dei cittadini, ma rendendo più solide le condizioni nelle quali essi possono comprendere, verificare e decidere. Il compito dell'Osservatorio sarà difficile proprio perché dovrà operare in uno spazio nel quale sicurezza e libertà, urgenza e prudenza, trasparenza e protezione delle fonti devono rimanere in equilibrio.

Le persone chiamate a partecipare dovranno contribuire non soltanto con il proprio sapere, ma con un metodo comune: centralità dei comportamenti e non delle opinioni, separazione tra rischio e prova, proporzionalità della pubblicazione, tutela dei dati, diritto di replica, revisione indipendente e disponibilità a correggere. In questo modo il White Paper annuale e i rapporti tematici potranno diventare strumenti realmente utili per Governo, Forze Armate, istituzioni, imprese, scuola e cittadini.

La qualità dell'iniziativa non sarà determinata dalla visibilità del lancio, dal numero delle segnalazioni o dalla severità del linguaggio. Sarà determinata dalla capacità di produrre evidenze affidabili, anticipare i rischi senza allarmismo, trasferire tempestivamente i casi alle autorità competenti e rendere comprensibili le contromisure. Chi sceglierà di aderire sarà chiamato a costruire questa credibilità nel tempo.

Principio guida

Conoscenza, non allarme. Orientamento, non censura. Raccomandazioni applicabili, non formule astratte. Indipendenza, prova e proporzionalità in ogni fase del lavoro.



FONDAZIONE OLIVETTI TECNOLOGIA E RICERCA – OLITEC

Osservatorio Nazionale sulla Proliferazione delle Armi Cognitive