PNR 2021-2027

Programma nazionale per la ricerca

GRANDE AMBITO DI RICERCA E INNOVAZIONE:

SICUREZZA PER I SISTEMI SOCIALI

Allegato esteso

Ministero dell'Università e della Ricerca

ESPERTI DEI GRUPPO DI LAVORO 3. SICUREZZA PER I SISTEMI SOCIALI

Sicurezza delle strutture, infrastrutture e reti: Angelo Masi (coordinatore), Iunio Iervolino, Massimo La Scala, Antonio Occhiuzzi, Antonio Pietrosanto, Roberto Ranzi, Enrico Zio

Sicurezza sistemi naturali: Alberto Guadagnini (coordinatore), Paola Francesca Antonietti, Francesco Castelli, Giovanni Crosta, Giancarlo Dalla Fontana, Rosanna De Rosa, Carlo Doglioni, Salvatore Grimaldi, Sandro Moretti, Tommaso Moramarco, Stefano Parolai, Roberto Zoboli

Cybersecurity: Rocco De Nicola (coordinatore), Giampaolo Bella, Francesco Buccafurri, Alfredo De Santis, Laura Emilia Maria Ricci. *Con contributi di: Nicola Blefari Melazzi, Stefano Bistarelli, Valentina Casola, Michele Colajanni, Marco Conti, Domenico Cotroneo, Ernesto Damiani, Sabrina De Capitani di Vimercati, Elena Ferrari, Sara Foresti, Francesco Palmieri, Paolo Prinetto, Pierangela Samarati, Aaron Visaggio.*

Roma, novembre 2020

L'allegato esteso include le riflessioni dei gruppi di lavoro di esperti nominati dal Ministero dell'Università e della Ricerca. Si tratta di un documento di approfondimento che esprime le opinioni degli esperti e che, dunque, non rappresenta una posizione ufficiale.

SOMMARIO

3. SICUREZZA PER I SISTEMI SOCIALI

La prosperità e il benessere dei cittadini sono fortemente legati alla sicurezza. La nostra vita quotidiana dipende da una grande varietà di servizi come l'energia, i trasporti, la finanza e la salute che si basano su infrastrutture sia fisiche che digitali. Parlare di sicurezza per i sistemi sociali non significa parlare solo di sicurezza personale, ma anche di protezione dei diritti fondamentali e di come porre le basi per la fiducia nella nostra società, nella nostra democrazia e nella nostra economia. Il danno potenziale di una minaccia alla sicurezza è amplificato dall'interdipendenza tra sistemi fisici e digitali: qualsiasi impatto fisico è destinato a colpire i sistemi digitali, mentre i cyber-attacchi ai sistemi informatici e alle infrastrutture digitali possono bloccare i servizi essenziali. La ricerca deve aiutare a identificare le nuove minacce e a capire il loro impatto sulla società in modo da proporre soluzioni innovative che possano mitigare i rischi nel modo più efficace.

L'Unione Europea ha dimostrato grande attenzione all'argomento inserendo il tema della sicurezza sia nel settimo Programma Quadro, sia in quelli successivi. In particolare, nel *position paper* "Orientations towards the first Strategic Plan for Horizon Europe" (dicembre 2019) del Programma Horizon Europe 2021-27, per il Cluster 3, "Civil security for Society", si legge: "... [il piano strategico] si prefigge di contribuire a proteggere l'UE e i suoi cittadini dalle minacce poste dalla criminalità e dal terrorismo (anche nell'ambiente cyber) e dagli impatti delle catastrofi naturali e di origine umana. .... la ricerca in materia di sicurezza fornisce gli strumenti per poter contrastare adeguatamente le minacce attuali, ...".

L'Ambito 3 "Sicurezza per i Sistemi Sociali", all'interno del quale si inserisce questo documento, si ricollega al Cluster 3 come evidenziato nel riquadro sottostante.

Ambiti Tematici (AT) - PNR 21-27	**Key Res. and Innov. Orientations - H-EU 21-27**
Sicurezza delle Strutture, Infrastrutture e Reti	Disaster-resilient societies
Sicurezza Sistemi Naturali	Protection and Security
Cybersecurity	Cybersecurity

Va evidenziato che il Cluster 3 include alcuni temi sicuramente collegati a problematiche di sicurezza, quali, a titolo di esempio: (*i*) *EU external borders*, (*ii*) *Protection of public spaces*, (*iii*) *Maritime security*, e *(iv) Fighting crime and terrorism*, che, in parte, vanno oltre gli scopi dei nostri gruppi di lavoro. In termini generali, le attività saranno coerenti con il contesto di riferimento del PNR 21-27, ossia i Sustainable Development Goals (SDGs), le Priorità espresse dalla nuova Commissione Europea e gli Obiettivi della Politica di Coesione 21-27.

Raggiungere tali obiettivi contribuirà ad accrescere la competitività del Paese in un contesto sempre più internazionale, con un significativo miglioramento nella quantificazione e nella comunicazione dei risultati ottenuti nella stima della pericolosità e del rischio e della relativa incertezza. In tale contesti, si ritiene utile sottolineare che le spese per ricerca su metodologie e tecnologie per la sicurezza rappresentano un importante investimento e sono funzionali ad aumentare la resilienza e la sostenibilità dei servizi e delle infrastrutture del nostro Paese ed ad accompagnare una strategia di sviluppo di breve e medio termine.

Nel seguito vengono delineati, in estrema sintesi, aspetti rilevanti ed obiettivi strategici dei tre ambiti tematici dell'ambito 3 del PNR 2021-27.

Sicurezza Strutture, Infrastrutture e Reti

Le attività di ricerca ed innovazione tecnologica di questo ambito tematico si collocano all'interno, ed intendono contribuirvi a livello nazionale, di politiche e direttive internazionali nel campo del Disaster Risk Management, tra le

quali in particolare il "Sendai Framework for Disaster Risk Reduction (2015-2030)" e lo "Union Civil Protection Mechanism".

Rispetto alla sicurezza delle sue strutture, infrastrutture e reti, va detto che l'Italia è una delle nazioni più esposte ai rischi naturali. In media, vi sono una ventina di terremoti distruttivi al secolo, che nel secolo scorso hanno causato oltre 100.000 vittime. Le eruzioni sono poco frequenti ma potenzialmente devastanti. Le frane note sono oltre 600.000, due ogni km^2. Le inondazioni sono comuni sia in ambiente di pianura che montano. Un terzo delle coste ha problemi di erosione. Infine, la posizione al centro del Mediterraneo rende l'Italia particolarmente sensibile ai cambiamenti climatici. Anche per questo, in Italia vi è una consolidata attenzione alla sicurezza e resilienza dell'ambiente costruito e delle infrastrutture, nonché del sistema di sistemi complessi, distribuiti e interdipendenti, che esse formano.

Le attività di ricerca devono, da un lato, tenere conto dei principali attributi della sicurezza e della resilienza, tra i quali: vulnerabilità dei sistemi, molteplicità dei pericoli di origine naturale e antropica, conoscenza imperfetta e/o incompleta (i.e., incertezza) di eventi pericolosi e dei loro impatti, robustezza e riparabilità/manutenibilità. Dall'altro lato, vanno considerate le principali complessità intrinseche a strutture, infrastrutture e sistemi a rete, derivanti principalmente da: molteplicità ed eterogeneità degli elementi (hard-cyber-human-ware) e delle tecnologie, dipendenze ed interdipendenze, estensione spaziale dei sistemi e delle conseguenze di eventuali disastri (potenzialmente intersettoriali e transnazionali), evoluzione nel tempo e vita utile residua, comparabilità dei rischi conseguenti a pericoli diversi, rapida evoluzione tecnologica.

Esigenze specifiche e temi di particolare rilevanza per il Paese, ai quali le articolazioni strategiche di ricerca dell'ambito tematico dedicano ampia attenzione, risultano essere: (i) sicurezza e robustezza del costruito, (ii) sicurezza e resilienza delle infrastrutture critiche, (iii) valutazione multi-hazard e multi-risk, (iv) analisi di sistemi complessi ed interdipendenti, (v) strategie di mitigazione delle conseguenze, (vi) consapevolezza e preparazione ai rischi delle comunità.

Sicurezza Sistemi Naturali

L'impatto economico e sociale legato alle perdite dovute a disastri naturali nel solo periodo 2009-2018 ha causato, a livello globale, il movimento di oltre 20 milioni di persone, con costi che hanno superato i 1500 miliardi di US$. È ampiamente riconosciuto che il rischio a maggior impatto è quello della mancata mitigazione degli effetti dei cambiamenti globali. L'impatto degli eventi naturali si manifesta sia in modo diretto che indiretto, essendo intimamente legato all'interazione con il tessuto antropizzato. Il raggiungimento di una mitigazione sostenibile dei rischi naturali richiede sforzi collaborativi inter- e multi-disciplinari e settoriali, per definire e valutare scenari di rischio affidabili e completi, nelle condizioni di incertezza tipica dei sistemi naturali stessi. In tale scenario, le incertezze di tipo strutturale e quelle sui dati di input influenzano la nostra capacità previsionale. L'incertezza dei dati è in parte aleatoria, e riflette la variabilità spaziale di flussi, stati e caratteristiche ambientali, e in parte epistemica. Quest'ultimo aspetto è legato all'osservazione che le basi dati disponibili per la caratterizzazione di sistemi complessi come quelli ambientali non sono esaustive. L'effetto dell'input del modello incerto è generalmente considerato essere fonte dominante di incertezza nella valutazione dei rischi associati ai sistemi naturali. L'incertezza strutturale di input e modello non è tuttavia indipendente e una sua appropriata quantificazione è riconosciuta essere alla base di una più solida conoscenza delle dinamiche evolutive del sistema Terra. L'acquisizione di nuove conoscenze mediante ricerche innovative permetterà lo sviluppo e l'evoluzione di modelli più affidabili per la valutazione della pericolosità, contribuendo a stime più affidabili delle conseguenze degli eventi, sia in tempo reale, che su diverse scale temporali. A tale scopo, lo sviluppo e la manutenzione di reti osservative, multi-parametriche ed integrate, diventa elemento critico per garantire l'analisi in tempo reale delle grandi e complesse basi dati relative alle diverse matrici ambientali. Obiettivi specifici, declinati nelle articolazioni sulle quali è strutturato l'ambito tematico, includono quindi: (*i*) l'avanzamento significativo delle conoscenze di base relative a processi naturali e la loro integrazione in modelli predittivi in condizioni di incertezza; (*ii*) il monitoraggio continuo, mirato e robusto dei sistemi naturali; (*iii*) la definizione di strategie moderne multi-rischio per la difesa da eventi naturali; (*iv*) lo sviluppo di strumenti di governance -e gestione delle interazioni tra rischi naturali e impatti antropici.

Cybersecurity

Blocco dell'operatività delle aziende, compromissione dei servizi delle infrastrutture critiche o di servizi essenziali, furto della proprietà intellettuale o di informazioni cruciali per la sopravvivenza di aziende e di asset nazionali, sono esempi di minacce cibernetiche. Gli attacchi informatici suscitano allarme, causano danni all'economia e mettono in pericolo l'incolumità dei cittadini quando colpiscono reti di distribuzione dei servizi essenziali come la sanità, l'energia, gli acquedotti, i trasporti. In Italia, interi settori di eccellenza, come la meccanica, la cantieristica, il made-in-Italy, il turismo, l'agro-alimentare, il farmaceutico e i trasporti, potrebbero subire pesanti ridimensionamenti di fatturato a causa di attacchi perpetrati da stati sovrani o da concorrenti sleali. Oggetto di attacco, ad esempio attraverso campagne di fake news, può essere anche il sistema politico e con esso la democrazia e i processi decisionali che ne sono alla base. Secondo alcune proiezioni, i costi delle violazioni dei dati raggiungeranno i 5.000 miliardi di dollari all'anno entro il 2024, in aumento rispetto ai 3.000 miliardi del 2015 (Juniper Research, The Future of Cybercrime & Security).

La cybersecurity non è però solo la definizione di strategie di difesa atte a contrastare gli attacchi, o mitigare il rischio, ma è anche un presupposto abilitante per la realizzazione di asset stabili e competitivi. Vi è infatti una crescente esigenza da parte di consumatori, cittadini, imprese e Pubblica Amministrazione, non solo di disporre di tecnologia IT sempre più avanzata e intelligente, ma anche di acquisire fiducia in tale tecnologia. Cybersecurity significa fornire "credibilità" al Sistema Paese, garantire vantaggi competitivi alle nostre imprese e fare in modo che le nuove metodologie, framework e tecnologie diventino volano per nuove imprese in un settore nella quale si manifestano gravi carenze di professionalità a livello mondiale. Per questo la ricerca di base e applicata in cybersecurity deve essere considerata una priorità. Obiettivi specifici, declinati nelle articolazioni sulle quali è strutturato l'ambito tematico, includono quindi: (*i*) individuazione tempestiva di possibili minacce e risposte agli attacchi cyber, (*ii*) garanzia di sicurezza di servizi erogati da sistemi digitali interconnessi tramite infrastrutture di comunicazione, (*iii*) avanzati strumenti di protezione delle risorse informatiche (iv) servizi di qualità al cittadino e alle imprese in termini di privacy, affidabilità ed efficienza (v) definizione di un framework di governo dell'ecosistema cyber basato sulla gestione del rischio, (vi) infrastrutture nazionali funzionali alla ricerca e allo sviluppo di servizi sicuri che garantiscano vantaggi economici e competitività.

3.1 Sicurezza delle strutture, infrastrutture e reti

Contesto attuale, motivazioni ed evoluzioni

L'Ambito Tematico "Sicurezza Strutture, Infrastrutture e Reti" (AT3.1) si colloca all'interno dell'Ambito "Sicurezza per i Sistemi Sociali" del PNR 21-27, corrispondente al Cluster 3 "Civil security for Society" del Programma Horizon Europe 21-27. Il position paper "Orientations towards the first Strategic Plan for Horizon Europe" del dicembre 2019 indica che il Cluster 3 mira a contribuire alla protezione della UE e dei suoi cittadini dalle minacce determinate da crimine e terrorismo, e dall'impatto di disastri naturali ed antropici.

Specificamente, l'AT3.1 intende promuovere attività di ricerca ed innovazione tecnologica che contribuiscano ad una efficace implementazione, a livello nazionale, di politiche e direttive internazionali nel campo del Disaster Risk Management (DRM), ed in particolare "Sendai Framework for Disaster Risk Reduction 2015-2030" e "Union Civil Protection Mechanism", oltre che "European Programme on Critical Infrastructure Protection", "EU Climate Adaptation Strategy", "EU environmental policies" (es. Seveso III, Flood Directives), "EU CBRN and Explosives Action Plans".

Allo stesso tempo, le attività di ricerca ed innovazione saranno coerenti con il contesto di riferimento generale del PNR21-27, ossia:

- i *Sustainable Development Goals* (SDGs) dell'Agenda 2030 dell'ONU
- la Strategia Nazionale per lo Sviluppo Sostenibile definita dal Ministero dell'Ambiente e della Tutela del Territorio e del Mare nel 2017
- le Priorità espresse dalla nuova Commissione Europea
- gli Obiettivi della Politica di Coesione 2021-27.

Dei diciassette SDGs previsti nell'Agenda 2030 almeno cinque (SDG7, 7, 9, 11 e 13) sono collegati all'AT 3.1 considerando la loro declinazione adottata anche dal nostro Paese che, in almeno due casi (SDG9 e SDG11), pone l'accento specificamente sulla resilienza di infrastrutture e comunità (Camera dei Deputati, giugno 2020).

Inoltre, considerando le Priorità espresse dalla nuova Commissione Europea (CE), nei documenti programmatici della Presidenza della CE, le linee di ricerca del PNR dovranno anticipare ed affiancare gli investimenti previsti per le infrastrutture, lo sviluppo sostenibile e la sicurezza che vanno delineandosi nei documenti preparatori del programma Horizon Europe, in particolare quelli relativi al Cluster 3, ma anche, in parte, ai Cluster 4 e 5.

Infine, con specifico riferimento alla Politica di coesione, va rilevato che tra i sei Obiettivi di Policy (OP), già nell'OP1 "*A low carbon and greener Europe" viene* dedicata particolare attenzione alla prevenzione e gestione dei rischi ed alla riduzione delle perdite. Nell'OP4 *"Promoting our European way of life"* tra gli obiettivi principali degli investimenti in ricerca ed innovazione vengono indicati, citando esplicitamente il Cluster 3, "*Improved disaster risk management and societal resilience*" e "*Improved security and resilience of infrastucture and vital societal functions*", quali impatti principali. In questo contesto ancora più prioritari per l'Italia saranno investimenti diretti a promuovere la resilienza ai rischi naturali, ad es. sismico e idrogeologico, con particolare attenzione per le infrastrutture critiche.

L'Italia è una delle nazioni più esposte ai rischi naturali, ed in particolare al rischio geologico, sismico, vulcanico, geomorfologico, idrologico, idraulico, meteorologico. In media, vi sono una ventina di terremoti con gravi conseguenze al secolo, che nel secolo scorso hanno causato oltre 100.000 vittime. Con riferimento agli ultimi anni, nel triennio 2016-2018 vi sono stati oltre cento terremoti con magnitudo uguale o superiore a 4.0, tre dei quali con magnitudo 5.5-5.9, e due superiori a 6 (ISTAT, 2020). Le eruzioni sono poco frequenti ma potenzialmente devastanti, anche nel breve termine. Le frane note sono oltre 600.000, due per ogni km² del territorio nazionale. Le inondazioni sono frequenti, sia nelle aree pianeggianti che in quelle montane. Un terzo delle coste ha problemi di erosione e le restanti in larga parte si trovano in condizioni di stabilità dovuta a interventi di protezione talvolta conflittuali con le dinamiche naturali. Infine, la posizione al centro del Mediterraneo rende l'Italia particolarmente sensibile ai cambiamenti climatici che possono portare ad estesi fenomeni di desertificazione, perdita di suolo e, per effetto

dell'innalzamento del livello dei mari, all'aumento della concentrazione salina nelle acque superficiali e sotterranee, accentuato da estrazioni idriche non più compensate dalle precipitazioni.

D'altra parte, in Italia vi è una consolidata attenzione alla sicurezza e resilienza dell'ambiente costruito e delle infrastrutture, nonché del sistema di sistemi complessi (strutture, reti di utilità e di servizi, infrastrutture strategiche e critiche, etc.), distribuiti e interdipendenti, che formano.

Da un lato, i principali attributi della sicurezza e della resilienza da considerare sono: (i) vulnerabilità dei sistemi intrinseca e dovuta a deterioramento, (ii) molteplicità dei pericoli di origine naturale e antropica, (iii) conoscenza imperfetta e/o incompleta (i.e., incertezza) riguardo al manifestarsi degli eventi pericolosi e dei loro impatti, (iv) robustezza e riparabilità/manutenibilità.

Dall'altro lato, vanno riconosciute le principali complessità intrinseche a strutture, infrastrutture e sistemi a rete, derivanti da: (i) molteplicità ed eterogeneità degli elementi (*hard-cyber-human-ware*) e delle tecnologie, (ii) dipendenze e interdipendenze (*sistemi di sistemi*), (iii) estensione spaziale fisica del sistema e delle conseguenze di eventuali disastri, potenzialmente intersettoriali e transnazionali (e.g., effetti domino e a cascata), (iv) evoluzione nel tempo e vita utile residua, (v) limitata disponibilità di risorse economiche per la sicurezza e resilienza, (vi) comparabilità dei rischi conseguenti a pericoli diversi, (vii) rapida evoluzione tecnologica (e.g., *energy transition, digitalization, robotization*).

Strumenti di analisi e valutazione, nonché tecnologie trasversali, vanno ricercati e sviluppati nelle aree scientifiche in cui risultano dominanti paradigmi quali: digitalization, *smart materials*, *data science, big data, machine learning, situation awareness, remote metering, fault diagnosis, robotica e droni, IoT, smart cities, smart grids, smart systems.*

Fondamentale, sia in fase di progettazione di nuove opere che di intervento su quelle esistenti, è la diponibilità di metriche quantitative per orientare la scelta tra diverse soluzioni possibili e comparare i livelli di sicurezza e di resilienza di sistemi diversi che svolgono le stesse funzioni. In tal senso, trasversale a tutte le attività di ricerca ed innovazione da sviluppare nell'AT3.1, appare la definizione di efficaci metriche della Sicurezza e del Rischio, ed in particolare: (i) metriche di resilienza, (ii) metriche per valutazioni multi-hazard e multi-risk (rischi naturali ed antropici) e relativi confronti, (iii) metriche per la valutazione di azioni di prevenzione strutturale e non-strutturale. Le metriche vanno finalizzate principalmente ad analisi del ciclo di vita e ad analisi costi-benefici multi-criterio e multi-livello, tenendo attentamente conto delle incertezze.

Per quanto riguarda il rischio sismico, l'Italia presenta un patrimonio edilizio ed infrastrutturale in larga parte costituito da costruzioni progettate secondo codici antisismici obsoleti, talvolta realizzate con materiali di scarsa qualità, e giunte in molti casi al termine della propria vita utile. In particolare, edifici storici ed edilizia popolare hanno in genere intrinseca vulnerabilità, come testimoniato da recenti eventi sismici, alla pari delle infrastrutture stradali per la gran parte frutto dello sviluppo italiano del dopoguerra. Pertanto, la valutazione e gestione della sicurezza del patrimonio storico e residenziale, il mantenimento in efficienza della rete infrastrutturale e degli edifici strategici costituiscono una priorità nazionale e, per certi versi, europea. Ciò richiede un'ottimizzazione degli sforzi economici per le manutenzioni e gli interventi ordinari/straordinari, per i quali risulta cruciale disporre di strumenti di valutazione rapida dello stato delle strutture, in modo particolare dopo un evento calamitoso come un sisma, nonché di un monitoraggio continuo dell'integrità di strutture e infrastrutture basato su misure del comportamento in servizio. In tale contesto, la capacità di fornire in tempi molto brevi (secondi/minuti) previsioni o early warning di eventi catastrofici, accompagnate dagli scenari di possibile distribuzione spaziale dell'impatto sia diretto (effetti dello scuotimento) che indiretto (fenomeni cosismici di liquefazione o frana) è fondamentale e richiede lo sviluppo di modelli evoluti per la quantificazione di pericolosità, esposizione e vulnerabilità.

Per quanto riguarda il rischio idrogeologico, il recente Rapporto SDGs 2020 per l'Agenda 2030 in Italia mette in evidenza come, in base alla mosaicatura effettuata da ISPRA delle aree a pericolosità idraulica elevata, media o moderata, il 10.4% della popolazione italiana sia esposto al rischio di danni alle persone (morti, dispersi, feriti, evacuati). Inoltre, il 2.2% della popolazione è esposto al rischio di frane in base alla mappatura delle aree a pericolosità elevata e molto elevata redatta dai Piani di Assetto Idrogeologico. Se i costi di riduzione della pericolosità idraulica e geologica sono molto elevati, e andrebbero concentrati soprattutto nel monitoraggio e nella manutenzione delle

opere esistenti (dighe, argini, opere di difesa e di sistemazione delle frane), margini di miglioramento significativi nella riduzione del rischio idrogeologico sono possibili agendo sull'esposizione, mediante una corretta pianificazione del territorio, e sulla vulnerabilità delle persone e cose, sia mediante prescrizioni edilizie che con una migliore informazione dei cittadini sui comportamenti da adottare in caso di calamità. A questo proposito la Campagna nazionale "Io Non Rischio" (www.iononrischio.it) promossa dal Dipartimento della Protezione Civile, insieme al Volontariato ed alla Comunità scientifica, costituisce un esempio imponente di come si possa operare per accrescere consapevolezza e preparazione dei cittadini in caso di eventi calamitosi, siano essi terremoti, alluvioni, etc.

Ancora, per quanto riguarda le infrastrutture energetiche e di trasporto, si rileva che negli ultimi 20 anni vi è stata una particolare attenzione alle infrastrutture vitali per la convivenza civile ed alla sempre maggiore dipendenza della società da esse. Ciò a causa di una serie di motivazioni, tra le quali: *unbundling* e *re-regulation* di alcuni settori e delle infrastrutture critiche, transizione energetica e decarbonizzazione, globalizzazione dei mercati, diffusione di ICT e sistemi di telecomunicazioni mobili, capacità tecnologica nella introduzione di *smart paradigms* (*smart grids, smart cities, smart sensors*), incremento dell'uso di servizi web-based. In particolare, l'evoluzione nella gestione delle infrastrutture energetiche da monopolistiche a *open-market* ha costituito un passo importante verso una maggiore efficienza dell'industria, correlata con una riduzione dei costi ed una maggiore centralità dell'utente oggetto di un numero maggiore di servizi user-friendly, ma ha anche esposto le infrastrutture critiche ad una serie di rischi mai sperimentati prima d'ora. Il vivere civile, sebbene possa apparire più robusto nei confronti di disturbi frequenti e di piccolo impatto, è risultato molto più vulnerabile rispetto a eventi a cascata, come dimostrato su scala globale a partire dalla stagione dei blackout elettrici del 2003 a valle della liberalizzazione del mercato elettrico. Questa specifica esperienza richiede che vengano individuate regole nuove per la protezione delle infrastrutture critiche.

In Europa, lo "*European Programme for Critical Infrastructure Protection (EPCIP)*" fissa il quadro generale per la protezione delle infrastrutture critiche per la UE. Le minacce non si limitano al terrorismo ma includono tutti i rischi inter-settoriali (attività criminali, pericoli naturali, etc.). In tal senso, sono state svolte molte attività sia di ricerca che per favorire un efficace coordinamento. Un caposaldo è costituito sicuramente dalla Direttiva 2008/114/CE che regolamenta l'individuazione e la designazione delle infrastrutture critiche europee. L'Allegato I di tale Direttiva riporta i settori ECI (European Critical Infrastructures), ossia Energia (elettricità, petrolio, gas) e Trasporti (stradale, ferroviario, aereo, marittimo e navigazione interna). Nel 2013, la CE, dopo aver valutato i progressi ottenuti nell'EPCIP, ha suggerito un nuovo Programma che dovrebbe condurre ad una fase più orientata a progetti concreti per il futuro. Questa fase si basa sul lancio di progetti pilota su quattro infrastrutture critiche: (i) la rete elettrica di trasmissione UE, (ii) la rete di trasporto del gas in UE, (iii) EUROCONTROL–the EU's Air Traffic Management, (iv) GALILEO.

La ricerca sulla Security in UE è stata già oggetto di finanziamento di numerosi progetti, ossia più di 150, anche in Horizon 2020. Il nuovo approccio sembra passare da progetti orientati dagli avanzamenti tecnologici (*technology-driven*) a progetti per la soluzione di problemi (*problem solving*), cercando un maggior coinvolgimento degli stakeholders dei vari settori di interesse. Tuttavia, sebbene sul tema specifico delle infrastrutture critiche sia stata sviluppata una significativa attività di ricerca negli ultimi 15 anni, in UE il trasferimento dei risultati verso applicazioni pratiche è ancora limitato. Questo spinge verso proposte di ricerca con TRL elevati. Con il PNR 2021-27 l'Italia ha la possibilità di guardare alle proprie specificità nel campo delle infrastrutture critiche anche favorendo un rapporto più ampio ed efficace con i principali stakeholders.

Vista l'ampiezza dell'AT3.1 appare opportuno proporre un elenco, ancorché non esaustivo, degli "oggetti" su cui opera l'AT3.1, suddivisi tra Strutture, Infrastrutture e Reti (Tabella 1).

STRUTTURE
- Costruito diffuso (es. edifici residenziali) - Manufatti singoli (es. Scuole, Ospedali) - Ponti - Gallerie - Opifici - Strutture sportive (Stadi, Palazzetti)

- Edifici storici e monumentali
INFRASTRUTTURE
- Infrastruttura urbana - Trasporto (es. aeroporti, eliporti, porti) - Acquedotti - Sistemi di drenaggio urbano (acque meteoriche e reflue) - Dighe e opere di sistemazione idraulica - Argini e opere di difesa idraulica - Impianti di potabilizzazione e depurazione delle acque reflue - Sistemi per la fornitura di energia elettrica - Sistemi per la fornitura di combustibili - Sistemi distribuzione prodotti (Supply Chain) - Sistemi di telecomunicazione - Sistemi satellitari - Portafogli di edifici residenziali - Reti di edifici strategici (es. sistema ospedaliero)
RETI
- Reti di trasmissione dati - Reti di trasporto e distribuzione acqua - Reti di trasporto e distribuzione di energia elettrica - Reti di trasporto e distribuzione di combustibili (oleodotti, gasdotti) - Reti di trasporto persone - Reti di trasporto merci - Reti satellitari - Reti di monitoraggio dei rischi ambientali e antropici

Tabella 1. Elenco (non esaustivo) delle Strutture, Infrastrutture e Reti su cui opera l'AT 3.1

Al tempo stesso, considerato che attività, obiettivi ed impatti previsti nella AT3.1 richiedono l'adozione di un approccio sistemico, accanto alle tre classi di "oggetti" su elencati, vanno considerati anche i seguenti Sistemi complessi:

- Comparti urbani (portafogli edifici a scala urbana, infrastrutture di edifici a scala urbana (es. ambiente costruito a scala urbana, reti di utilità a scala urbana (distribuzioni), infrastrutture di trasporto e approvvigionamento a scala urbana, infrastrutture di servizi a scala urbana).
- Comunità regionali (portafogli edifici a scala regionale, infrastrutture di edifici a scala regionale, reti di utilità a scala regionale (distribuzioni), infrastrutture di trasporto e approvvigionamento a scala regionale, infrastrutture di servizi a scala urbana).
- Comunità nazionali (ambiente costruito, reti di utilità a scala nazionale (distribuzioni), infrastrutture di trasporto e approvvigionamento a scala nazionale, reti di servizi a scala nazionale).
- Sistemi interdipendenti alle varie scale spaziali.
- Sistemi interdipendenti a varie scale temporali (e.g., pre-crisi, durante evento catastrofico, gestione delle emergenze, recupero nel medio e lungo termine).

Rilevanza rispetto alle transizioni ambientale, digitale, economica, energetica e sociale

La ricerca sulla sicurezza di strutture, infrastrutture e reti deve tenere conto di alcune rapide transizioni in atto, ossia quella ambientale, digitale, economica, energetica e sociale.

Tra le **transizioni ambientali** quella climatica è senz'altro quella che più attira l'attenzione della società civile essendo ormai scientificamente accertato come l'aumento delle temperature, in accelerazione dalla seconda metà del secolo scorso, sia anche di origine antropica. Il suo effetto è già osservabile, ad esempio, nella diminuzione della disponibilità delle risorse idriche superficiali e sotterranee, nella crescita della domanda irrigua delle colture e nell'aumento del livello dei mari, con impatto non trascurabile sulle infrastrutture di adduzione, invaso e distribuzione idrica e sulle opere di difesa costiera. Si deve rispondere all'incremento della domanda irrigua per effetto del riscaldamento globale con l'efficientamento delle reti di adduzione consortili, monitorando e riducendo le perdite lungo le adduttrici e le reti di distribuzione, il miglioramento tecnologico delle tecniche irrigue (microirrigazione, irrigazione di precisione, monitoraggio con droni e satellitare), e delle pratiche colturali.

L'aumento delle temperature ha anche un impatto sulla sicurezza della disponibilità di energia sul mercato elettrico che deve adattarsi alla modificata distribuzione temporale della domanda di energia il cui picco sta migrando dal periodo invernale a quello estivo, per le necessità del raffrescamento degli edifici. La politica di transizione energetica dall'uso di fonti fossili a quelle rinnovabili, imboccata con convinzione dall'Europa e dall'Italia già dal programma 20-20-20, deve ora tradursi in una accelerazione dei processi in atto per centrare l'obbiettivo della riduzione delle emissioni del 40% entro il 2030 e quello, ancora più ambizioso, della neutralità dell'impatto antropico sul clima entro il 2050, uno dei principi cardine del Green New Deal europeo.

Per migliorare la sicurezza di strutture e infrastrutture nel contesto della variabilità climatica e dell'aggiornamento delle conoscenze e misure disponibili sulle catastrofi naturali è necessario sviluppare la ricerca di base e applicata su criteri di progettazione più cautelativi per alcune strutture e infrastrutture rispetto alle sollecitazioni temibili, da un lato, e agli aggiornamenti normativi, dall'altro. La richiesta sociale di maggiore sicurezza si è tradotta in un aggiornamento dei criteri di progettazione e in un innalzamento dell'intensità delle sollecitazioni e tempi di ritorno di progetto in molti settori (Norme Tecniche sulle Costruzioni del 2018, Norme Tecniche sulle Dighe del 2014, Direttiva Alluvioni 2007/60/EC, D.Lgs. 49/2010, Leggi regionali sull'invarianza idraulica dei sistemi di drenaggio urbano), con ricaduta sui costi necessari per l'adeguamento e la riabilitazione strutturale difficilmente sostenibili in un contesto di ristrettezza delle disponibilità di investimento. L'individuazione delle priorità di intervento sarà possibile a seguito di importanti investimenti nella ricerca e innovazione in sistemi di monitoraggio in situ e remoti per edifici, ponti, dighe, argini, oleodotti, gasdotti, linee elettriche, etc.. Infine, vanno ulteriormente sviluppate soluzioni integrate e sostenibili per favorire un ampio programma di riqualificazione del patrimonio edilizio ed infrastrutturale esistente che coniughi sicurezza ed efficientamento energetico, tenuto conto che il fabbisogno energetico degli edifici determina circa il 40% del consumo totale di energia.

La **transizione digitale** e l'innovazione tecnologica, associate al paradigma di Industria 4.0, stanno permeando una buona fetta del nostro sistema imprenditoriale nel settore dell'automazione industriale, della robotica (secondi soli alla Germania per installazione di nuovi robot e ben al di sopra della media mondiale), dell'intelligenza artificiale. Come rilevato dal 53° rapporto del CENSIS sulla situazione sociale del paese (2019) circa la metà delle imprese italiane negli ultimi cinque anni ha fatto investimenti in tecnologie e trasformazioni digitali. Questa spinta innovativa, che si è tradotta nella fitta rete di incubatori e acceleratori di imprese innovative, va assecondata e sostenuta anche nel settore della sicurezza delle strutture, infrastrutture e reti ad esempio nel monitoraggio e controllo delle strutture civili, delle reti di trasporto, degli impianti di produzione e distribuzione dei combustibili e dell'energia, di distribuzione idrica, delle grandi strutture e infrastrutture come i ponti, le dighe, le arginature fluviali, i porti e le opere di difesa delle coste.

Anche la **transizione energetica** trova un contesto sociale ricettivo e favorevole al progressivo abbandono delle fonti fossili e alla decarbonizzazione che trova sostegno nel PNIEC, Piano Nazionale Integrato per l'Energia e il Clima del dicembre 2019, che prevede risorse per la ricerca, l'innovazione, la competitività nel settore. In tal senso, sono state messe in campo una serie di importanti misure per il conseguimento degli obiettivi tra cui, in particolare, il Fondo per la Ricerca di sistema elettrico ed il Fondo per interventi e misure per lo sviluppo tecnologico e industriale. Inoltre, la non-programmabilità e la disomogeneità spaziale delle fonti rinnovabili richiede lo sviluppo di studi e ricerche per adeguamenti della infrastruttura energetica sia con interventi 'hard' (es. realizzazione di sistemi accumulo dell'energia e il potenziamento e ammodernamento delle reti su diversa scala spaziale), che con applicazione di tecnologie digitali per il controllo della sicurezza e l'utilizzo efficiente dell'energia. Anche la ricerca sulla gestione dei

sistemi idroelettrici dovrebbe andare nella direzione auspicata dal PNIEC di un incremento dell'utilizzo degli impianti di generazione-pompaggio esistenti, grazie anche ai rinforzi di rete pianificati, nel nord Italia, oltre a nuovi impianti della stessa tipologia. Studi sono già in corso ma approfondimenti sono necessari per verificare l'utilità dello sviluppo di nuove forme di accumulo dell'energia per garantire la sicurezza strategica e la resilienza del Paese a fronte di situazioni di shock energetico estreme. Legate ad esse sono nuove tecnologie di conversione dell'energia elettrica verso/da altri vettori energetici, tecniche di immagazzinamento sotto forma di materia (note con l'acronimo P2X). Nuove tecnologie dovranno anche essere sviluppate per superare la carenza di inerzia della infrastruttura elettrica a fronte del *phase out* di grandi centrali fossili (*virtual inertia, fast frequency regulation*) e per il controllo anche rapido del carico. La collocazione mediterranea del nostro Paese favorisce lo sviluppo e la diffusione di sistemi di generazione di energia che sfruttino le maree, il moto ondoso, le correnti marine, passando dalla fase di ricerca e sviluppo dei prototipi, nella quale la ricerca italiana teorica e applicata ha assunto posizioni di rilievo internazionale, alla produzione industriale su larga scala. Per raggiungere questo obbiettivo è auspicato un maggiore coordinamento tra i centri di ricerca e i laboratori del settore, anche realizzati in mare aperto, con esempi di eccellenza nel Meridione d'Italia.

Le trasformazioni **sociali ed economiche** con la richiesta di riqualificazione strutturale del patrimonio edilizio e di maggiore comfort abitativo continuano, nonostante la decrescita demografica, a sostenere il consumo di suolo con un aggravio dell'esposizione e della vulnerabilità di persone e beni ad eventi geofisici estremi, se il nuovo assetto territoriale non viene progettato prestando attenzione alla sicurezza. Un maggiore accento, sostenuto dalla ricerca in ambito urbanistico-territoriale, sulla rigenerazione urbana e riqualificazione dell'ambiente costruito piuttosto che sull'edificazione ex-novo dovrebbero rallentare, se non invertire, la tendenza in atto e salvaguardare il patrimonio ambientale costituito dal paesaggio agricolo, asse portante della catena agroalimentare, dai parchi e le aree protette, risorse essenziali per il sostegno dell'economia turistica.

Obiettivi 2021-2027

Considerando il contesto attuale, sia nazionale che internazionale, e considerando in modo particolare le specificità ed esigenze italiane, si identificano alcuni temi/obiettivi che si ritengono strategici per l'AT3.1, ossia:

- **sicurezza e robustezza del costruito;**
- **sicurezza e resilienza delle infrastrutture critiche;**
- **valutazione multi-hazard e multi-risk;**
- **analisi di sistemi complessi ed interdipendenti;**
- **strategie di mitigazione delle conseguenze;**
- **consapevolezza e preparazione ai rischi delle comunità.**

Specifica attenzione va anche rivolta al monitoraggio e analisi dei dati per diagnostica e valutazione predittiva dei rischi.

Per conseguire tali obiettivi strategici multidisciplinari appare particolarmente importante promuovere la creazione ed il potenziamento di **infrastrutture di ricerca**, favorendo la sinergia tra laboratori esistenti, nonché lo sviluppo delle risorse umane dedicate alla ricerca di base e applicata, attraverso **dottorati di ricerca** di ampiezza sistemica e multi-disciplinare, anche di tipo industriale.

Principali attività da svolgere, obiettivi specifici ed impatti attesi relativi ai suelencati obiettivi strategici, anche operando in stretta interconnessione con altri Ambiti Tematici, vengono dettagliatamente descritti al par. 4, dove vengono presentate le Articolazioni di ricerca considerate strategiche per l'AT3.1.

Le attività di ricerca dovranno determinare l'avanzamento delle conoscenze di base (TRL basso-medio) verso l'applicazione e il trasferimento tecnologico (TRL medio-alto), con il coinvolgimento delle pubbliche amministrazioni e delle comunità professionali ed imprenditoriali.

L'integrazione tra ricerca di base e industriale, il trasferimento di conoscenze dalla ricerca fondamentale a quella applicata, richiedono infrastrutture di ricerca condivise, oggi largamente deficitarie nel sistema di ricerca italiano, e

sempre più necessarie anche rispetto agli sviluppi della ricerca in UE, in particolare nel programma Horizon 21-27. È indispensabile lo sviluppo di una strategia condivisa che eviti duplicazioni e favorisca aggregazioni di dimensioni adeguate per la creazione di reti infrastrutturali nelle quali si collochino gli investimenti di ordine superiore, particolarmente necessari per gli ambiti più innovativi e avanzati. Esempi importanti, attualmente esistenti nei settori della Terra solida e delle aree marine, sono EPOS ed EMSO, due iniziative infrastrutturali europee ERIC a guida italiana che sono una grande opportunità e rafforzano il ruolo della ricerca italiana in alcuni settori strategici. In tal senso, grazie alla presenza in Italia di laboratori avanzati per la sperimentazione di materiali e strutture, che operano a servizio delle pubbliche amministrazioni e in ambito industriale, va promossa la realizzazione di una grande infrastruttura di ricerca nel campo dell'ingegneria strutturale e sismica che metta ancor più a sistema e valorizzi reti ed esperienze già esistenti. Inoltre, la centralità mediterranea dell'Italia indica anche l'opportunità di sviluppo di una rete tra i Laboratori di idraulica e idraulica marittima e costiera con vasche e canali per modelli 3D e 2D di grandi dimensioni. È necessario che tale infrastruttura tenga conto delle realtà esistenti in termini di grandi laboratori, consorzi e centro di competenza sugli stessi temi o affini.

In UE la Commissione europea ha creato lo *European Reference Network for Critical Infrastructure Protection (ERNCIP)* per promuovere lo sviluppo di soluzioni per la sicurezza che siano innovative, qualificate, efficienti e competitive, mettendo in rete le capacità diffuse in Europa. Si tratta di una rete di laboratori per effettuare ricerche sui temi della sicurezza e della resilienza, e sperimentare nuovi modelli, metodologie, tecnologie e sistemi di diagnostica. Alcuni programmi di ricerca nazionali, nel tempo, hanno consentito di "aggregare" centri di ricerca con finalità che includono le tematiche della sicurezza delle infrastrutture critiche. È il caso, ad esempio, del fondo per la Ricerca di Sistema elettrico a cui partecipa, oltre RSE, ENEA, CNR, il sistema delle università italiane con una serie di accordi quadro per la condivisione di laboratori e risorse scientifiche. Sono operanti su questi temi anche consorzi interuniversitari come ENSIEL, partecipato dal MiSE e dal MUR e controllato dal MEF, organismo di riferimento nazionale per gli stakeholder italiani del settore, e come Me.S.E. che raggruppa le Università italiane attive sul tema delle Metriche e delle Tecnologie di Misura sui Sistemi Elettrici. Sulla base di queste premesse, si potrebbe promuovere un centro simile al ERNCIP in Italia che possa coordinare una organizzazione "a rete" dei laboratori operanti nei vari settori disciplinari e che possa interagire più facilmente con la rete europea nell'ambito della sicurezza delle infrastrutture critiche.

Grande importanza ha la formazione di dottori di ricerca, anche tramite il potenziamento dei dottorati industriali, capaci di disegnare, sviluppare e implementare ricerca innovativa e sviluppo tecnologico in un contesto fortemente multi- e inter-disciplinare, anche per soddisfare le crescenti esigenze della pubblica amministrazione. Per una tale formazione, prioritario è mettere a fattor comune le diverse competenze necessarie, attraverso la creazione di reti di dottorati nazionali e internazionali basate sulla formazione attraverso la ricerca. Dottorati multidisciplinari sulla gestione integrata dei rischi (multi-hazard e multi-rischio) di sistemi complessi e interdipendenti, e che mettono in opera le nuove tecnologie e metodologie (anche di analisi dei dati, intelligenza artificiale, machine learning), rappresentano una grande opportunità di sviluppo dell'alta formazione. Per un più efficace trasferimento delle conoscenze, anche alla società civile, è indispensabile che tali programmi di dottorato forniscano anche competenze adeguate nel campo della comunicazione e della disseminazione.

Vanno poi potenziati strumenti normativi e finanziari che, superando il precariato, favoriscano la mobilità bidirezionale dei ricercatori (mobilità inter-universitaria, tra Enti di ricerca, tra Enti e Atenei, e tra istituzioni pubbliche e industria), ai fini della creazione di una rete dinamica ed efficace di sviluppo e diffusione delle conoscenze e competenze.

ARTICOLAZIONI

L'AT3.1 prevede le seguenti quattro Articolazioni strategiche di ricerca:

- **Analisi e Valutazione dei Rischi e della Resilienza**
- **Metodi, Tecniche e Tecnologie per il Monitoraggio e la Prevenzione dei Rischi**
- **Gestione dei Rischi e della Resilienza**

- **Sicurezza e Resilienza per la Società e lo Sviluppo Sostenibile**

Nel seguito, vengono presentate le quattro Articolazioni, i cui elementi essenziali sono stati forniti nella Scheda sintetica dell'AT 3.1.

Per ogni Articolazione, dopo una descrizione degli aspetti generali, vengono riportati **Obiettivi** ed **Impatti** principali, oltre ad indicare le possibili **Interconnessioni** con altri Ambiti Tematici ed alcuni ***Key Perfomance Indicators*** che possano consentire di valutare la qualità dei risultati delle attività di ricerca e degli impatti raggiunti.

Va rilevato che, all'interno delle quattro Articolazioni strategiche, possono essere individuate specifiche linee di ricerca, un elenco (non esaustivo) delle quali è riportato in **Appendice 1** (Tabella A.1).

Articolazione 1. Analisi e valutazione dei rischi e della resilienza

Le strutture, infrastrutture e reti, oggetto di questo ambito tematico, sono costituite da molti componenti di diverso tipo (hardware, human e cyber) che interagiscono tra loro in configurazioni fisiche e logiche progettate per fornire determinate funzioni e servizi in maniera ottimale, affidabile e sicura. L'analisi e la valutazione dei rischi e della resilienza sono funzionali a garantirne la sicurezza in tutte le fasi del loro ciclo di vita.

Le configurazioni di strutture, infrastrutture e reti sono organizzate gerarchicamente (sistemi, sottosistemi, componenti). Durante il loro ciclo di vita, vengono sottoposte ad aggiornamenti, migliorie, integrazioni con nuove tecnologie, estensioni per soddisfare nuove e crescenti richieste di servizio, con modifiche anche sostanziali dettate dalle evoluzioni della società, dell'economia, delle normative e della politica, nonché dalle continue e sempre più rapide innovazioni tecnologiche.

In questo scenario di evoluzione e innovazione, le strutture, infrastrutture e reti sono diventate sempre più interconnesse. La loro vulnerabilità ed il rischio di cedimento, guasto e danno, sia individuale che sistemico, a seguito di eventi calamitosi (inclusi quelli dolosi), destano una crescente preoccupazione da parte della Società intera. Prendendo ad esempio l'ambito energetico, gli scenari di decarbonizzazione previsti dalla politica di transizione energetica intrapresa in Italia e gli ambiziosi obbiettivi del Green New Deal europeo richiedono nuove soluzioni sia fisiche che digitali, per la gestione delle fonti non programmabili, e risorse energetiche distribuite e soluzioni tecnologiche per dare flessibilità alla infrastruttura tra cui l'accumulo (storage elettrochimico, Power to Gas, impianti idroelettrici di generazione-pompaggio, etc.). La necessità di un uso efficiente delle risorse energetiche, ad es. nei sistemi multi-generazione (multi-generation systems), orienta la tecnologia verso infrastrutture energetiche integrate che includono elettricità, gas naturale, reti di teleriscaldamento/raffrescamento, idrogeno e, quindi, una rapida evoluzione verso sistemi multi-energy, in cui differenti vettori energetici interagiscono tra loro in modo sinergico. La necessità di garantire l'approvvigionamento energetico in condizioni di sicurezza e la possibilità tecnologica di convertire più fonti di energia primaria in forme di energia destinata a più servizi energetici interdipendenti richiedono di considerare nuovi scenari di evoluzione di sistemi energetici multi-vettore. Tale contesto di sviluppo integrato richiede un'attenta analisi e considerazione delle implicazioni sulla sicurezza nella progettazione e operazione di sistemi finora concepiti e operati in maniera largamente indipendente, adottando adeguate metodologie di analisi sia dei rischi ai quali i sistemi sono esposti che della resilienza, metodologie attualmente non disponibili e che vanno, dunque, sviluppate.

Più in generale, nello scenario di aumentata integrazione dei sistemi e di crescente domanda di servizi in un mercato deregolamentato, i margini di sicurezza coi quali le strutture, le infrastrutture e le reti sono state progettate potrebbero essere insufficienti per assorbire gli stress, attesi e inattesi, che impattano su di loro ed emergono dalla sovrapposizione di molteplici effetti individuali che incidono collettivamente su di esse. Ciò può determinare grandi incertezze nella caratterizzazione dei processi che portano al fallimento, cedimento, danno di questi sistemi complessi, e nella determinazione delle conseguenze che ne derivano attraverso le interconnessioni e interazioni dei molteplici elementi costitutivi. L'esperienza testimonia come le strutture, infrastrutture e reti possano essere soggette a condizioni di forte stress che portano a comportamenti fortemente non-lineari con cedimenti a livello di sistema, in conseguenza di perturbazioni relativamente piccole e locali che poi si propagano a cascata attraverso dipendenze e interdipendenze, con impatti, anche transnazionali, di grande entità.

D'altra parte, l'importanza e la potenziale criticità dei sistemi oggetto di questo ambito tematico portano alla necessità di proteggerli dai pericoli ai quali sono esposti e garantirne adeguate proprietà di resilienza. Vanno certamente considerati tutti i molteplici pericoli attualmente già noti, di origine sia naturale che antropica (compresi gli attacchi malevoli, sia fisici che cyber), ma anche quelli potenzialmente emergenti da nuove tecnologie e nuovi usi, nonché quelli futuri prevedibili. La diversa natura e la complessità dei pericoli ai quali i sistemi sono esposti fanno sì che i classici approcci all'analisi di rischio basati su metodi riduzionisti siano destinati a fornire una imprecisa e incompleta descrizione dell'eterogeneità intrinseca a questi sistemi e delle associate complessità strutturali, dinamiche ed operazionali. L'analisi di questi sistemi non può essere svolta solo con i metodi classici di decomposizione del sistema e di analisi delle logiche di funzionamento. Ad integrazione dei metodi esistenti, sono necessari nuovi approcci metodologici e modellistici capaci di fornire una descrizione completa della complessità di questi sistemi, tenendo conto dell'eterogeneità dei loro componenti, delle loro interazioni, delle dipendenze e interdipendenze e considerando le inevitabili incertezze dell'analisi. Nuovi inquadramenti sono necessari per integrare diversi metodi di analisi che guardino al sistema dalle diverse prospettive (topologiche e funzionali, statiche e dinamiche, etc.) che ne caratterizzano e influenzano il funzionamento e il fallimento. Dunque, è necessario adottare un approccio sistemico e olistico, di integrazione di diversi metodi.

Riguardo all'approccio sistemico, le ricerche dovranno portare allo sviluppo di metodologie di analisi quantitativa in grado di tenere in debito conto le caratteristiche di complessità e interdipendenza di questi sistemi, che ne fanno dei sistemi di sistemi eterogenei, con componenti fisiche, cyber e umane che interagiscono tra loro, il cui fallimento (accidentale o causato) può propagarsi a cascata generando guasti, danni e perdite nei sistemi interconnessi. Per tale motivo, un aspetto cruciale da tenere in considerazione nelle analisi è il ruolo della produzione e della condivisione delle informazioni sullo stato dei sistemi e della loro interoperabilità, che può influenzarne fortemente la resilienza.

Un altro aspetto da considerare è il coinvolgimento delle comunità potenzialmente esposte alle conseguenze di un incidente o di un disastro, nonché il loro contributo alla resilienza. In questo, le tecnologie di comunicazione e informazione (es. i social media) possono avere un ruolo significativo, ma non è ancora chiaro come i contenuti e le dinamiche di informazione e comunicazione (e le relative tecnologie a supporto) influenzino il processo di costruzione della resilienza in una comunità di persone coinvolte in un'emergenza, in particolare a seguito di un disastro. Creare e condividere informazioni è un processo molto complesso, fortemente dipendente dal contesto e influenzato da fattori sociali, culturali, economici e tecnici. Come altrettanto impegnativo è lo sviluppo di modelli di comportamento sociale che permettano di prevedere il comportamento di fronte agli eventi e quindi il contributo umano alla resilienza dei sistemi. Come tenere conto di questi aspetti nelle analisi di rischio e nelle valutazioni di resilienza è un tema prioritario da considerare.

Obiettivi

Per la analisi e valutazione dei rischi e della resilienza delle strutture, infrastrutture e reti, occorre sviluppare metodi adeguati alla loro complessità, per:

- la rappresentazione del sistema;
- la modellazione del sistema;
- la quantificazione del modello per il calcolo di indicatori caratteristici (metriche) di rischio e resilienza;
- la rappresentazione e la propagazione delle incertezze.

Data la natura dei sistemi oggetto dell'analisi e valutazione, la modellazione deve includere ed integrare:

- attributi fisici, quali la configurazione, il comportamento dinamico, le dipendenze tra componenti e le interdipendenze tra sistemi, il livello di pervasività dei sistemi di monitoraggio, ecc.;
- attributi operativi e di gestione, inclusi quelli di comunicazione e controllo, i fattori umani e organizzativi, gli aspetti logistici, ecc.;
- indicatori di performance funzionale e sicurezza, inclusi affidabilità, disponibilità, manutenibilità, capacità di gestione dell'emergenza e di risposta ai disastri, ecc.;
- attributi economici, quali i costi di ciclo vita, i driver del mercato, la business continuity, l'integrità degli asset, ecc.;

- attributi sociali, inclusi la percezione e la risposta degli attori coinvolti, la comunicazione e informazione, l'offerta e domanda di servizio, ecc.;
- attributi ambientali, inclusi gli eventi climatici, l'inquinamento, la sostenibilità, ecc.

La modellazione deve consentire l'analisi e la valutazione dei sistemi e delle loro complessità da diverse prospettive, integrando:

- Metodi di modellazione topologica, tipici dell'analisi di sistemi complessi e delle reti, della teoria dei grafi, della fisica statistica. Questi metodi offrono lo strumento per descrivere la connettività dei componenti eterogenei in un sistema complesso e le interdipendenze tra sistemi, consentendo di analizzarne gli effetti sulla funzionalità del sistema, sulla propagazione a cascata di guasti e danni, sulla resilienza. Consentono inoltre di identificare gli elementi critici del sistema perché centrali nella connettività per il suo funzionamento o la propagazione del suo fallimento.
- Metodi logici di analisi di sistema, quali gli alberi gerarchici, i diagrammi di influenza, le reti bayesiane. Questi metodi consentono di rappresentare e valutare le logiche di funzionamento e fallimento di sistemi complessi e a rete, e di identificare le combinazioni di fallimenti di componenti eterogenei (hardware, software e human) che causano la perdita di funzionalità del sistema.
- Metodi di modellazione funzionale, basati su funzioni di trasferimento, modelli input-output e parametrici, modelli ad agenti etc., per descrivere quantitativamente la dinamica di operazione tra gli elementi eterogenei (hardware, software e human) interagenti nel sistema complesso, con gli altri sistemi e con l'ambiente, da cui emerge la dinamica del sistema stesso.
- Metodi di modellazione fisica, basati su modelli di flusso, modelli meccanicistici (anche "first-principles") per descrivere quantitativamente i processi fisici che avvengono nel sistema complesso.

Da un lato, i suddetti metodi vanno ulteriormente sviluppati e, dall'altro, vanno completati con tecniche in grado di:

- identificare in maniera efficiente possibili pericoli ed eventi inattesi (i cosiddetti "cigni neri"), derivanti dalla complessità del sistema stesso, dalla sua evoluzione e dal suo utilizzo futuro. A tale scopo sono necessari metodi integrati di simulazione stocastica (per la considerazione dell'incertezza sull'accadimento e sullo svolgimento degli eventi di danno e sullo sviluppo delle loro conseguenze) e deterministica (per la fenomenologia fisica della risposta del sistema agli eventi) e di *design of experiment* con tecniche statistiche e data-driven di intelligenza artificiale, che consentano di generare in maniera computazionalmente efficiente molteplici potenziali futuri scenari, identificando quelli critici per la sicurezza del sistema;
- valutare il rischio aggregato derivante dai molteplici pericoli ai quali una struttura, rete o infrastruttura è esposta;
- valutare le metriche di rischio e resilienza in maniera adattiva, incorporando le informazioni, le stime e le previsioni sullo stato di degrado e cedimento dei componenti il sistema che derivano dall'analisi statistica dei dati di campo e dall'analisi di prognostica dei dati di monitoraggio.

Per la quantificazione, in particolare, appare rilevante che le metriche utilizzate consentano di valutare gli impatti negativi dovuti a riduzioni della sicurezza di esercizio e della resilienza, e l'inserimento dei risultati all'interno delle analisi decisionali per la pianificazione degli interventi a potenziamento della sicurezza e resilienza dei sistemi, delle reti e delle infrastrutture critiche. Sebbene alcuni passi siano stati mossi in qualche settore (elettricità, gas) in termini quantitativi ed economici, le metriche di resilienza non appaiono consolidate. Inoltre, sono necessari studi per estendere e particolarizzare le metriche e le metodologie di analisi a tutti i settori critici, affinché siano in grado di considerare le specificità fisiche e operative dei diversi settori nel computo del "costo" e del "valore" della sicurezza e della resilienza, ai fini della definizione delle priorità di intervento.

D'altro lato, la complessità e la dimensione delle strutture, infrastrutture e reti richiedono l'integrazione, in una visione tipica di "sistemi di sistemi", di tecniche di co-simulazione a diverse scale di dettaglio e analisi spaziali mediante tecniche geostatistiche. La sfida principale per i metodi sarà riuscire a considerare le interrelazioni tra i sistemi fisici (es. elettricità, gas, acqua) e i sistemi immateriali come i mercati, il sistema bancario, gli effetti sociali e macroeconomici, etc.

In conclusione, di seguito una lista (non esaustiva) di argomenti (elencati non in ordine di importanza) per potenziali ricerche utili all'analisi e valutazione del rischio e della resilienza di strutture, infrastrutture e reti, argomenti che, in alcuni casi, si pongono in stretta relazione con le altre Articolazioni di ricerca (in particolare le Articolazioni 3. Gestione dei Rischi e della Resilienza, e 4. Sicurezza e Resilienza per la Società e lo Sviluppo Sostenibile):

- Metodi di valutazione del rischio da pericoli multipli, inclusi i guasti e danni fisici, gli eventi naturali estremi, gli attacchi cyber e fisici (Methods for multi-hazard risk assessment, including failures, extreme natural events, cyber and physical attacks)
- Metodi di valutazione del rischio aggregato da pericoli multipli (Methods for multi-risk aggregation from multiple hazards)
- Metodi di analisi quantitativa della resilienza di sistemi di sistemi (Methods for the quantitative analysis of systems of systems resilience)
- Metodologie per lo sviluppo di modelli fisici e data-driven, previsionali dell'evoluzione di scenari incidentali e disastri naturali (First-principle and data-driven models for scenario generation)
- Metodi di analisi di rischio integrata mediante simulazione stocastica e deterministica dell'evoluzione di scenari incidentali e disastri naturali (Integrated deterministic and probabilistic risk assessment by joint simulation of the accident scenarios and natural disasters)
- Metodi di analisi di rischio adattiva basata su stima e previsione delle condizioni del sistema (Condition-based adaptive risk assessment)
- Metodi di analisi dell'incertezza nelle valutazioni di rischio e resilienza di una struttura, rete, infrastruttura (Methods of uncertainty analysis in risk and resilience assessment of a structure, network, infrastructure)
- Metodi di analisi di sensitività per l'identificazione dei fattori e parametri che maggiormente influenzano il rischio e la resilienza di una struttura, rete, infrastruttura (Methods of sensitivity analysis for the identification of the factors and parameters that most influence the risk and resilience of a structure, network, infrastructure)
- Approcci di progettazione basata sulla resilienza (Resilience-based design approaches)
- Metodi di valutazione della distribuzione sociale della resilienza e dei fattori che vi concorrono (Methods for social distribution of resilience)
- Metodi di analisi delle interrelazioni tra mercati, aspetti sociali e sicurezza delle infrastrutture critiche (Methods for the analysis of the interrelations among market and social aspects with the safety of critical infrastructures)
- Metodi di analisi e valutazione della resilienza di comunità (Methods of community resilience analysis and assessment)
- Analisi e valutazione del livello e comportamento etico di resilienza di comunità (Community resilience ethics analysis and evaluation)
- Metodi e modelli per la valutazione del contributo alla resilienza ai disastri, proveniente dal coinvolgimento e cooperazione della comunità (Methods and models for the assessment of community engagement and cooperation for resilience building)
- Metodi per la valutazione del ruolo delle tecnologie per la comunicazione e informazione nella resilienza delle comunità e nella gestione delle emergenze generate da incidenti e disastri (Methods for the assessment of information technologies for community resilience and disaster response management)
- Metodi di analisi quantitativa del costo e valore della resilienza (Methods for the analysis of cost and value of resilience)
- Metodi per la definizione e valutazione degli obbiettivi di resilienza (Resilience goals definition and assessment)
- Metodologie per la definizione degli aspetti regolatori e di risk governance (Risk governance methods)
- Modelli strategici e geopolitici per la resilienza (Strategic and geo-political models for resilience)

Impatti

Da quanto sopra esposto, si evince che l'analisi e la valutazione del rischio di strutture, infrastrutture e reti richiedono estensioni significative degli approcci classici di analisi del rischio ed importanti sviluppi di nuove metodologie per ottenere una maggiore confidenza nelle soluzioni di prevenzione di rischi multipli e di risposta a eventi inattesi

(inclusi quelli dolosi), considerando adeguatamente le complessità, le interdipendenze e le incertezze caratteristiche di questi sistemi di sistemi così vitali per il funzionamento della nostra società.

Pertanto, gli impatti attesi dalle ricerche sono riconducibili allo sviluppo di modelli, metriche, metodi, piattaforme e strumenti di calcolo per l'analisi olistica dei pericoli ai quali le strutture, infrastrutture e reti sono esposte, per la valutazione del loro rischio e resilienza al fine di fornire informazioni quantitative di supporto, anche in tempo reale, alle scelte decisionali relative alla progettazione di soluzioni di prevenzione e azioni di mitigazione delle conseguenze, a favore della crescita della resilienza dei sistemi e delle comunità coinvolte.

Con riferimento agli Impatti Attesi previsti nel Cluster 3 del programma Horizon, l'impatto relativo alla presente Articolazione ricade principalmente in "*Security threats are more effectively addressed thanks to better cross-cutting knowledge across different areas of security, enhanced implementation of the research and innovation cycle and improved uptake*". Lo statement associato è *"Improved security and resilience of infrastructure and vital societal functions.*".

Interconnessioni con altri Ambiti Tematici

La complessità dei problemi legati alla sicurezza delle strutture, infrastrutture e reti trova una evidente esemplificazione considerando le interazioni con i temi legati alla sicurezza dei sistemi naturali con riferimento ai disastri, come per esempio quelli di origine sismica, di particolare rilevanza sul territorio nazionale italiano.

Va precisato che i terremoti sono fenomeni naturali, il cui studio "fenomenologico" coinvolge l'AT Sicurezza dei sistemi naturali, ma la protezione e la resilienza delle strutture, infrastrutture e reti relativamente agli effetti dei terremoti è tema proprio di questa AT, considerando ciò che attiene alle alle analisi e valutazioni di rischio e resilienza, alla loro gestione, etc. A tale riguardo, la stessa definizione di resilienza va specificamente contestualizzata, considerandone aspetti caratteristici quali:

- eventi sostanzialmente ingovernabili (es. il fenomeno sismico naturale);
- sistemi parzialmente ingovernabili (strutture e infrastrutture fisiche, per le quali generalmente i concetti di osservabilità e controllabilità della Teoria dei sistemi e del controllo trovano un'applicazione molto parziale, se non nulla);
- componenti e comportamenti umani molto differenziati (regolatori, decisori, soccorritori, cittadinanza) per i quali i livelli di Human Reliability assumono tutta la gamma dei possibili valori prevedibili, atteso l'elevatissimo numero di soggetti potenzialmente coinvolti.

L'analisi e la valutazione dei rischi e della resilienza vanno in questo caso specificamente contestualizzate e adattate in considerazione dei tre aspetti sopra citati (fenomeni naturali, sistemi infrastrutturali e comportamento umano). Il complesso sistema di sistemi va quindi analizzato mediante tecniche che siano in grado di prendere in considerazione e "misurare" grandezze che differiscono non solo nelle unità di misura ma anche in termini di ambiti culturali e scientifici di riferimento.

Dal lato antropomorfo, invece, un problema che si pone nella sicurezza delle infrastrutture e dell'industria in generale è dato dalla cybersecurity del sistema OT/IT (Operational Technology/Information Technology). Nella società moderna, la cybersecurity ha ormai assunto un ruolo vitale per qualsiasi tipo di attività industriale, comprese le infrastrutture critiche. L'industria si trova a operare in un contesto di rischio continuamente e rapidamente mutevole, con l'esigenza di mantenere e migliorare al contempo i propri prodotti e servizi da offrire all'utilizzatore finale. Inoltre, con il sistema regolatorio in continua evoluzione, nuove opportunità di business guidate da tecnologie innovative potenzialmente "disruptive" (inclusi i servizi cloud e l'Internet of Things (IoT)) impattano profondamente sulla struttura stessa del business e dell'industria, creando forti interconnessioni con sistemi distribuiti operati, gestiti e di proprietà di terzi. L'industria ha accelerato significativamente la sua evoluzione verso il digitale, con una forzata accelerazione durante la recente pandemia, aumentando la sua dipendenza da asset e componenti cyber (sistemi di trasmissione e controllo, dispositivi intelligenti, etc.) per l'operazione dei suoi impianti di produzione e la gestione della fornitura dei propri servizi. Questi asset e componenti cyber sono cruciali per la sicurezza, affidabilità ed efficienza dei sistemi, delle infrastrutture e delle reti industriali e di servizio. D'altra parte, presentano anche serie

sfide in quanto è necessario saper affrontare il rischio di attacchi cyber, che si affiancano ai pericoli derivanti da errori cyber degli operatori, da guasti fisici dei componenti, da eventi naturali e a quelli che emergono dalla complessità dei sistemi di sistemi e dall'interazione dei molteplici attori sul sistema. I problemi di cybersecurity vanno affrontati in maniera integrata con quelli di sicurezza e resilienza, per poter efficacemente prevenire attacchi cyber e mitigarne gli impatti sulla sicurezza fisica umana, funzionale del sistema, ambientale, sociale. Se in passato il progetto, lo sviluppo, l'operazione ed il mantenimento di un impianto, sistema, struttura, infrastruttura, consideravano aspetti di pericolo/rischio legati solo all'ingegneria di sistema e processo, ora è necessario includere anche gli aspetti ed elementi connessi ai servizi e alle tecnologie di cybersecurity interconnessi con i sistemi e processi ingegneristici con il risultato che i nuovi impianti, i nuovi sistemi, le nuove infrastrutture potrebbero essere significativamente diverse come configurazione, capacità e vincoli.

In questo contesto, proprio la resilienza dovrebbe essere il concetto driver integrante per garantire la continuità di servizio e business in quanto la resilienza integra gli attributi di affidabilità, sicurezza, security dei processi e dei servizi, e consente di definire un processo di continuo miglioramento a supporto della continuità di servizio e business. In quest'ottica, la resilienza non va vista come puro aspetto tecnico ma deve coinvolgere l'organizzazione intera in un approccio al problema che va affrontato combinando le tecniche di cybersecurity con l'ingegneria di sistema e i processi operativi, per essere preparati ad affrontare mutazioni di contesto e, in particolare, a resistere e rispondere con efficacia e rapidità a eventuali eventi distruttivi.

Per quanto detto, dunque, sono da incentivare ricerche mirate alle necessità specifiche delle reti e dei sistemi industriali digitalizzati ed automatizzati, nelle più recenti configurazioni che poggiano massicciamente sul ricorso alla misura ed al controllo distribuiti ed all'IoT. Per questi sistemi è necessario sviluppare metodi autodiagnostici ed autoriparatori (self diagnosis and accommodation) per la *resilience by design* considerando la stretta correlazione delle funzioni per la gestione dei sistemi fisici di automazione con il funzionamento dei molteplici sistemi cyber di comunicazione.

Key Performance Indicators

La qualità dei risultati della ricerca e degli impatti raggiunti andrà valutata mediante indicatori che tengano conto dei seguenti aspetti principali:

- Evidenza del valore scientifico della proposta e dei proponenti, attraverso la considerazione di valori bibliometrici standard e al riconoscimento a livello internazionale.
- Evidenza del contributo al valore competitivo per l'industria nazionale.
- Evidenza, in coerenza con lo scenario internazionale e la sua evoluzione, del contributo alla piattaforma collaborativa, anche trans-nazionale, per la protezione e resilienza delle infrastrutture critiche, a supporto degli operatori e delle autorità pubbliche responsabili della protezione degli asset e della loro resilienza, rispetto a rischi e malfunzionamenti di varia natura.
- Evidenza del coinvolgimento concreto anche delle piccole e medie imprese e delle start-up nelle attività di ricerca e nel beneficio derivante dai suoi risultati e dall'accesso alle tecnologie e ai dati, promuovendo l'inclusione e gli ambienti collaborativi.
- Interdisciplinarietà della ricerca per la progettazione e la pianificazione di interventi di potenziamento delle infrastrutture, con dimostrata capacità di descrivere ed analizzare le interdipendenze settoriali.

Articolazione 2. Metodi, tecniche e tecnologie per il monitoraggio e la prevenzione dei rischi

Le attività di monitoraggio, controllo e prevenzione sono essenziali per garantire la sicurezza di strutture, infrastrutture e reti, e per misurare i livelli di resilienza raggiunti. I metodi e le tecnologie per il monitoraggio sono fortemente legati agli avanzamenti tecnologici del settore, ai sistemi di controllo e di gestione finalizzati alla prevenzione dei rischi e agli obiettivi che, allo stato attuale, sempre più tendono a superare una mera stima di vulnerabilità e vanno nella direzione della valutazione dei livelli di resilienza dei sistemi oggetto dell'osservazione. È

necessaria una intensa attività di ricerca per coniugare il raggiungimento di nuovi obiettivi con le possibilità metodologiche e tecnologiche innovative disponibili nei settori del monitoraggio e analisi dei dati, della diagnostica e previsione, del controllo e della gestione di sistemi complessi.

Una peculiarità dell'Italia consiste nel **patrimonio storico e architettonico** e nella obsolescenza di una certa parte del costruito che rende tale patrimonio fortemente vulnerabile, come viene puntualmente dimostrato in occasione di gravi eventi climatici e sismici che hanno provocato e provocano danni alle cose (collassi, crolli, fratture, frane e cedimenti) e perdita di vite umane. Questa condizione motiva una particolare attenzione per la ricerca di nuove tecniche di monitoraggio e diagnostica in questo settore.

Si osserva, inoltre, che negli ultimi 20 anni, nel nostro Paese, è stata posta una particolare attenzione alle **infrastrutture critiche** vitali per la convivenza civile di un paese, e alla sempre maggiore dipendenza della società da esse a causa di una serie di motivazioni:

- *Unbundling* e *deregulation* in diversi settori infrastrutturali
- Globalizzazione dei mercati
- *Energy transition* e *Green Deal*
- Diffusione di ICT e sistemi di telecomunicazione mobili
- Capacità tecnologica nella introduzione di *smart paradigms* (es. *smart grids, smart cities, smart working)*
- Incremento dell'uso di servizi web-based.

L'evoluzione nella gestione delle infrastrutture dei servizi di pubblica utilità da monopolistiche a open-market ha costituito un passo importante verso la ricerca di una maggiore efficienza dell'industria e dei servizi, correlata con una riduzione dei costi ed una maggiore centralità dell'utente oggetto di un numero maggiore di servizi *user-friendly*, ma ha anche esposto le infrastrutture critiche ad una serie di nuove minacce. Questo è accaduto per la maggiore complessità dovuta al nuovo scenario socio-economico e tecnologico caratterizzato da interazioni reciproche tra differenti infrastrutture, e da una aleatorietà introdotta dall'apertura ai mercati che si sostituivano ad una gestione integrata verticalmente con pianificazione centralizzata. La stagione dei blackout elettrici del 2003 su scala globale a valle della liberalizzazione del mercato elettrico ne appare come la relativa dimostrazione. Questi fenomeni socio-economici hanno incrementato la complessità di gestione delle infrastrutture critiche. L'intero vivere civile, sebbene possa apparire più robusto nei confronti di disturbi frequenti e di piccolo impatto, risulta, oggi, molto più vulnerabile rispetto a situazioni di emergenza. Inoltre, alcune scelte politiche di lungo periodo adottate a livello europeo e globale comportano una vera e propria rivoluzione tecnologica, come nel caso della digitalizzazione e la transizione energetica, che implicano fenomeni di rapida trasformazione di alcune infrastrutture che, se non opportunamente governati, possono renderle maggiormente vulnerabili e meno resilienti. Proprio questa esperienza dimostra la necessità di sistemi di monitoraggio e prevenzione dei rischi che tengano conto della pluralità delle numerose entità coinvolte, dei legami intersettoriali, delle aleatorietà che ne conseguono e delle tecnologie emergenti. Inoltre, una visione ingegneristica della resilienza mira a preservare le funzionalità critiche delle strutture e infrastrutture in presenza di gravi perturbazioni ed eventi inattesi, minimizzando il degrado delle prestazioni ed assicurando, allo stesso tempo, una evoluzione quanto più graduale possibile, nonché garantendo un rapido e completo recupero delle prestazioni iniziali grazie all'utilizzo di soluzioni tecnologiche che tengano presente la specificità dei sistemi da gestire. È necessario, pertanto, sviluppare tecnologie di monitoraggio e controllo in grado di permettere alle infrastrutture di assorbire l'impatto di un evento e recuperare nel più breve tempo possibile le condizioni normali di funzionamento. Queste tecnologie devono consentire di garantire al meglio la capacità di sopravvivenza (Survivability) e di autoriparazione (Self-healing) del sistema.

Sistemi innovativi di monitoraggio e controllo, anche adattativi, potranno scaturire da avanzamenti sia metodologici (identificazione di modelli, tecniche diagnostiche per "recovery" e "accommodation"), sia tecnologici (misure in tempo reale, comunicazioni wireless, calcolo ad alte prestazioni, tecniche di intelligenza artificiale, ecc.). Tali innovazioni dovranno essere mirate a consentire azioni di monitoraggio e controllo non solo nella fase di prevenzione degli eventi dannosi, evidenziando le condizioni di elevata vulnerabilità, ma anche nelle fasi di emergenza e di ripristino delle prestazioni iniziali, al fine di garantire una maggiore resilienza dei sistemi controllati. È chiaro da

questa visione che, in ognuno degli obiettivi della resilienza, la funzione di monitoraggio associata ad una appropriata azione di controllo e gestione del rischio assume un ruolo centrale.

Bisogna osservare, inoltre, che la risposta di alcune infrastrutture critiche a perturbazioni esterne è fortemente influenzata dal comportamento dinamico che, in alcuni casi, può essere particolarmente rapido. Durabilità, *Survivability* e proprietà di *self-healing* sono fattori fortemente influenzati dalla risposta dinamica del sistema. Inoltre, le conseguenze dei disturbi sono fortemente dipendenti dalla loro dinamica temporale e, pertanto, questo aspetto deve essere considerato all'interno delle analisi e valutazioni di resilienza. Quindi, sistemi di monitoraggio sufficientemente evoluti e tali da "catturare" la dinamica di interesse, interpretare i fenomeni in corso, predirne l'evoluzione e fornire dati alle funzioni di controllo assumono un ruolo di interesse per l'attività di ricerca. Il potenziale di recupero dell'infrastruttura dipende dalla capacità di riconoscere il fenomeno in corso, prevederne l'evoluzione e riorganizzarsi per fronteggiarlo e superarlo. Per alcuni sistemi (ad es. l'infrastruttura elettrica) ciò deve avvenire in tempi molto rapidi, compatibili con l'evoluzione dei fenomeni e a volte con azioni su area geografica estesa (anche continentale), ponendo problematiche che richiedono nuova attività di ricerca.

In ambito industriale e per le infrastrutture critiche vanno sviluppate tecnologie per il controllo della resilienza (*Resilience control systems*) per garantire un accettabile livello di sicurezza ed un livello di prestazione più elevato possibile in risposta ad eventi poco frequenti ma ad alto impatto. La ricerca dei prossimi anni deve, quindi, individuare le metodologie, i componenti, le tecnologie e le strategie di monitoraggio in grado di "osservare e riconoscere" i fenomeni critici sulle necessarie scale temporali e spaziali, e garantire la necessaria flessibilità, capacità di controllo e rapidità di azione tali da permettere un adattamento ai grandi eventi perturbanti ed un rapido ritorno alle prestazioni pre-disturbo.

Obiettivi

Obiettivo generale è lo sviluppo di nuove conoscenze che forniscano metodi e tecnologie in grado di far fronte a scenari che coinvolgono sistemi complessi ed interdipendenti, soggetti a nuove minacce derivanti da modificate condizioni ambientali e da contesti geopolitici, socio-economici e tecnologici in rapida evoluzione. Le soluzioni che dovranno essere studiate e sviluppate nel periodo 2021-2027 dovranno essere in grado di dare risposte mirate per le singole strutture e infrastrutture, che tengano conto delle specificità di ogni settore e, allo stesso tempo, siano in grado di riconoscere e controllare le interazioni tra realtà fisiche e funzionali molto diverse.

Le problematiche di ricerca nel campo dei sistemi di monitoraggio innovativi di strutture, infrastrutture e reti sono numerose ed interdisciplinari e sono caratterizzate da aspetti sia teorico-analitici, sia tecnologici. Le direttrici principali della ricerca dovranno portare alla realizzazione di sistemi di monitoraggio distribuiti, sia fissi che mobili e robotizzati (droni, rover, etc.) che siano in grado, con crescente autonomia, di produrre e trasferire con continuità informazioni prelevate in accordo alle caratteristiche dei sistemi sotto osservazione ed ai loro modelli analitici. Sistemi che siano in grado di apprendere autonomamente, estraendo conoscenza dai dati acquisiti, per migliorare la sensibilità, la selettività e le capacità diagnostiche e previsionali. A tal fine, direttrici della ricerca dovranno essere indirizzate in particolare verso tecniche e tecnologie di posizionamento ottimo dei sensori guidate da obbiettivi di riduzione del rischio e aumento della resilienza, di robotizzazione per la mobilità di misura, di "sensor data fusion" intelligente, di analisi della influenza del decadimento progressivo dei sensori e della probabilità di "missed detection", con conseguente aumento del rischio e diminuzione della resilienza.

Per il monitoraggio, controllo e prevenzione del rischio di strutture, infrastrutture critiche interdipendenti e di sistemi complessi vanno sviluppate soluzioni basate sulla integrazione di:

- tecnologie e sistemi di monitoraggio, in-situ e da remoto,
- tecniche di *data analysis* applicate a big data, per la rilevazione anticipata di pericoli incipienti, la diagnostica di cause di pericolo, la previsione dell'evoluzione del pericolo
- sistemi e strumenti per l'individuazione di possibili condizioni di criticità di strutture e infrastrutture.
- Sistemi di nuova generazione capaci di integrare i concetti di "gemello digitale" ed "intelligenza artificiale" con quelli di "sistemi di misura in tempo reale" e "strumentazione virtuale".

Una ulteriore direttrice dovrà portare allo studio della propagazione dell'incertezza di misura e del livello di confidenza delle conoscenze statistiche, ad esempio rispetto al rischio sismico e a fenomeni meteorologici estremi per strutture ed infrastrutture, nei sistemi multi-sensore, in situ e remoti, per il monitoraggio e previsione di eventi metereologici estremi finalizzati tra l'altro alla riconfigurazione preventiva di reti e sistemi complessi. In particolare, andrà sviluppata la ricerca su sistemi innovativi sia di monitoraggio in continuo su infrastrutture come elettrodotti, sistemi di adduzione, trasporto e distribuzione dei fluidi (acquedotti, oleodotti, gasdotti) sia di monitoraggio puntuale di possibili situazioni critiche in singole strutture (ponti, edifici, dighe, arginature). Andranno anche sviluppati i metodi di le associate tecniche di analisi di big data (basate anche su intelligenza artificiale e machine learning) per rilevazione e previsione della evoluzione di degradi e comportamenti anomali, ai fini del loro controllo mediante manutenzione su condizione e predittiva.

Nel seguito si riportano alcuni contesti e relativi obiettivi specifici da considerare nell'ambito dei sistemi di monitoraggio, controllo e prevenzione dei rischi.

Sicurezza e conservazione di edifici storici, siti archeologici e monumenti

Gli edifici storici, siti archeologici e monumenti rappresentano una parte fondamentale del patrimonio culturale e dell'identità stessa dell'Italia, pertanto il loro recupero e la loro protezione e conservazione hanno valenze culturali, sociali ed economiche di evidente importanza. Tale patrimonio architettonico risulta, tuttavia, fortemente vulnerabile, come viene puntualmente dimostrato in occasione di gravi eventi climatici e sismici che hanno provocato e provocano danni alle cose (collassi, crolli, fratture, frane e cedimenti) e perdita di vite umane.

Per fronteggiare efficacemente tali minacce la ricerca deve risolvere una serie di problemi, tra i quali:

- lo sviluppo di modelli per la valutazione dello "stato di salute strutturale" delle costruzioni storiche e la previsione della sua evoluzione, che tengano conto della propagazione delle incertezze di misura e di conoscenza nelle valutazioni del rischio da pericolo sismico ed eventi metereologici estremi;
- la definizione di idonee strategie di analisi della risposta strutturale, specie sotto l'effetto del sisma e di eventi metereologici estremi;
- lo studio di approcci al consolidamento delle strutture, che siano in grado di garantire i necessari livelli di sicurezza senza determinare alterazioni della costruzione, incompatibili con i principi del restauro;
- lo sviluppo di sistemi di monitoraggio basati su sensori e reti di comunicazione non intrusive, misure senza contatto e a distanza, reti wireless, tecniche "low power" per lo sviluppo di "smart sensor" e batterie di dimensioni sempre minori, e delle associate tecniche di analisi di big data (anche traendo beneficio dagli sviluppo dell'intelligenza artificiale e del machine learning) per rilevazione e previsione dell' evoluzione di degradi e comportamenti anomali, ai fini del loro controllo mediante manutenzione su condizione e predittiva.

Transizione energetica e infrastrutture collegate

L'Italia persegue da tempo il più ampio ricorso a politiche che garantiscano sicurezza energetica, tutela dell'ambiente, accessibilità dei costi dell'energia. I piani di sviluppo del sistema energetico italiano prevedono un processo di decarbonizzazione dell'energia che si inserisce, a pieno titolo, nelle politiche europee del *Clean Energy package* e del *Green Deal*. Una specificità italiana è caratterizzata da una politica mirata ad una rapida transizione dai combustibili tradizionali alle fonti rinnovabili, promuovendo l'abbandono del carbone per la generazione elettrica a favore di un una quota crescente di rinnovabili e gas naturale. In questa logica, si inserisce il PNIEC (Piano Nazionale Integrato Energia e Clima) che prevede come obiettivo al 2030 una quota di fonti rinnovabili del 30% sui consumi finali lordi ed un contributo pari al 55% nella produzione di energia elettrica. La concretizzazione di tale transizione esige ed è subordinata sia alla programmazione e realizzazione degli impianti sostitutivi e delle necessarie infrastrutture che ad un cambio di paradigma nella tecnologia in grado di garantire adeguati livelli di sicurezza e resilienza della infrastruttura energetica. Le principali problematiche di sicurezza che possono derivare da tale scenario, e che la ricerca deve affrontare, sono: la riduzione della adeguatezza (*adequacy*), *over-generation* delle centrali termoelettriche, riduzione della Inerzia del sistema elettrico, congestioni delle reti di trasporto dell'energia, ripidità della rampa serale elettrica, problemi di qualità del servizio.

Pertanto, vanno sviluppati metodi innovativi per il monitoraggio ed il controllo della sicurezza dei sistemi energetici interconnessi su scala nazionale e continentale, tenendo conto delle incertezze connaturate al nuovo contesto e della necessità di rendere più flessibili gli impianti convenzionali.

I temi di ricerca potranno essere rivolti alla definizione di metodologie per la valutazione della sicurezza e della vulnerabilità, nuovi componenti e apparati per le reti, gestione, monitoraggio e controllo delle reti di trasporto dell'energia, strumenti di modellazione e simulazione per l'analisi di scenari elettrici, energetici, ambientali, sistemi per il monitoraggio e controllo di fenomeni a rapida evoluzione, sistemi di controllo ed apparati per garantire la flessibilità delle reti, metodi e modelli di intelligenza artificiale per l'analisi di big data a fini di valutazione e previsione, nuove soluzioni organizzative ed architetture dei sistemi energetici, smart grids, smart meters, coinvolgimento degli utenti attivi, approcci collaborativi tra operatori di rete.

Nel nuovo assetto di transizione energetica, un aspetto qualificante per la prevenzione dei rischi è lo sviluppo di *smart, secure and more resilient energy systems* per favorire la capacità di monitoraggio, di interoperabilità dei sistemi, di coordinamento degli operatori di sistema sia a livello di trasporto a lunga distanza che di distribuzione. Sui livelli di distribuzione più bassi, generalmente costruiti nella logica *fit and forget*, appare fondamentale garantire l'osservabilità ed una capacità di controllo degli stessi.

Nel settore elettrico, nuovi avanzamenti tecnologici e regolatori permettono di prevedere un sempre maggiore coinvolgimento dei *prosumer* (*pro*ducer + con*sumer*) e degli utenti attivi in nuovi mercati partecipando con la produzione diffusa e la flessibilità del carico anche ai servizi ausiliari di rete utili a garantirne la sicurezza. Il coinvolgimento di questi nuovi attori e la possibilità di monitoraggio, misura e controllo diffusi fornirà nuove opportunità, da cogliere a livello scientifico, nella capacità di anticipare, assorbire e recuperare situazioni di contingenza, fornire nuovi servizi per l'energia e la sicurezza nella logica della *Transactive energy* (anche con tecnologia blockchain), realizzazione di nuovi schemi di distribuzione più resilienti ed affidabili (es. sviluppo delle *networked microgrids, Virtual Power plants, Vehicle to Grid, Home Energy Management Systems (HEMS)*) ma anche servizi innovativi per i livelli di distribuzione più bassi quali *blackstart generation* e *restoration capability* tramite risorse distribuite.

Nuove minacce ambientali, antropiche, sociali

Le strutture, infrastrutture critiche e reti richiedono una drastica rivisitazione delle tecnologie per la sicurezza in relazione ad una serie di nuove minacce dovute ai rapidi cambiamenti climatici e ambientali, a fattori antropici e sociali quali terrorismo fisico e cyber o crisi socio-sanitarie inattese come, ad esempio, la recente pandemia che ha fatto lavorare alcune infrastrutture critiche in condizioni nuove e mai esplorate in precedenza con effetti significativi sulla sicurezza, sull'organizzazione della manutenzione e sui mercati correlati (es. dell'energia).

In tali casi, la prevenzione del rischio e la resilienza dei sistemi a fronte delle contingenze di origine naturale ed antropica necessitano di un articolato e ben coordinato complesso di analisi teoriche e modellistiche che permettano l'utilizzo delle architetture concettuali e dei modelli utili a valutare gli scenari di minacce, vulnerabilità e risposte con un approccio probabilistico, e di essere preparati e pronti (*preparedness e readiness*) in risposta a scenari ad alto impatto e bassa frequenza. In questo contesto assume un rilievo particolare anche la ricerca di metodologie di rilevazione, diagnostica e previsione di anomalie e danni, di componenti e materiali innovativi orientati all'incremento della resilienza delle strutture e infrastrutture necessarie per fare fronte alle mutate sollecitazioni ambientali, ai fenomeni estremi ed alla mitigazione dei loro effetti. Rilevante in tal senso è il settore della diagnostica e prognostica, ovvero la possibilità di disporre di tecniche in grado di valutare lo stato dei componenti, e anticiparne l'evoluzione, consentendo un intervento precoce riducendo la probabilità di disservizi estesi (manutenzione su condizione e predittiva). In relazione agli eventi estremi, possibili tematiche da sviluppare sono: metodologie mirate al superamento degli attuali approcci deterministici, studio dei fenomeni meteorologici con sovraccarichi di neve e ghiaccio e sviluppo di materiali e tecniche di monitoraggio e controllo (ad es. su linee elettriche aeree), fenomeni di accumulo di contaminanti sugli isolatori dei sistemi elettrici e diagnostica, effetto delle ondate di calore e assenza di piogge, sismi e inondazioni e loro effetto sulla resilienza e *fragility* delle infrastrutture, modellazione, diagnostica e previsione dei fenomeni di invecchiamento di isolamenti dielettrici solidi. Di notevole interesse anche i temi della

sicurezza e monitoraggio nei confronti di attacchi fisici e cyber su infrastrutture critiche e gli effetti di pandemie su condizioni di funzionamento anomale di alcune infrastrutture dovute a basso carico ad interazioni negative con altri sistemi, quali ad esempio i mercati, a problematiche connesse al personale e alla manutenzione degli impianti.

Sistemi satellitari e "Aeromobili a Pilotaggio Remoto", GPS

Un ruolo di rilievo nei sistemi di monitoraggio potranno avere sia i sistemi satellitari sia gli aeromobili a pilotaggio remoto (APR) o "*Unmanned Aerial Vehicle*" (UAV). A satelliti di piccola taglia a basso costo oppure ad APR dedicati potrà essere affidata la sorveglianza delle infrastrutture critiche da minacce naturali, surriscaldamenti e punti caldi, attacchi criminali e furti, sicurezza degli assets, controllo della vegetazione e manutenzione delle servitù di elettrodotto. Sviluppi di tali funzionalità basate sulle immagini provenienti da varie forme di veicoli autonomi devono derivare da nuove ricerche in alcuni settori, tra i quali: "*Image Processing and Recognition*"; auto-calibrazione di sistemi di ricostruzione 3D; batterie di scarso peso, grande capacità e contenuto tempo di ricarica; sistemi di ricarica wireless, reti di telecomunicazioni satellitari e terrestri, tecnologie satellitari al servizio di infrastrutture multiple (elettricità, acqua, gas, agricoltura, etc.) al fine di una ottimizzazione degli investimenti; sistemi di *Early Warning*.

La disponibilità di sistemi di posizionamento globale (GPS) apre la strada ad una serie di applicazioni di rilievo nel settore della sicurezza delle strutture ed infrastrutture. Queste tecnologie e l'attività di ricerca correlata permettono la realizzazione di sistemi "*Wide Area Measurements and Control*" che si sono dimostrati validi strumenti per scongiurare effetti a cascata su area geografica estesa (anche continentale) per fenomeni a dinamica veloce con capacità di rapida propagazione (ad esempio nel caso di oscillazioni inter-area nei sistemi elettrici). A questo proposito, appare rilevante l'individuazione di metodologie e applicazioni per l'utilizzazione della tecnologia GALILEO per il monitoraggio delle grandi infrastrutture e per la ricostruzione di eventi con *time stamp* aventi valore legale in UE (ad esempio, per la ricostruzione a fini legali di blackout generalizzati delle infrastrutture elettriche tramite sincrofasori).

Sicurezza di infrastrutture idrauliche

Gli investimenti fatti a partire dalla prima metà del secolo scorso in importanti infrastrutture idrauliche (dighe, sistemi acquedottistici, arginature) hanno portato molte di queste opere alla conclusione del loro ciclo di vita. Molte strutture e infrastrutture sono state progettate disponendo di serie storiche brevi, non sempre in grado di cogliere né la naturale variabilità delle forzanti idrometeorologiche, né, tanto meno, i successivi cambiamenti di origine climatica e antropica, come le modifiche di uso del suolo o gli sviluppi normativi. Si pone pertanto il problema dell'adeguamento delle opere di sbarramento alle prescrizioni delle Norme Tecniche sulle Dighe (Regolamento Dighe) del 2014, sviluppando la ricerca di base, numerica e sperimentale sul monitoraggio strutturale, sulla diagnostica e sulla previsione del comportamento idraulico delle dighe e delle opere di scarico. Inoltre, l'obsolescenza delle adduttrici e delle condotte di distribuzione idrica rende urgente lo sviluppo di tecniche di monitoraggio, diagnostica, previsione e controllo delle pressioni e delle perdite nelle reti di distribuzione con l'obbiettivo di ridurre le perdite, oggi molto elevate, migliorare la sicurezza degli impianti acquedottistici e la loro capacità di soddisfare la domanda, in continua crescita anche per effetto del riscaldamento globale. Andrà promossa la ricerca sull'integrazione di interventi di controllo dei deflussi meteorici con soluzioni 'Nature-Based' (NBS) e tradizionali per tendere all'invarianza idraulica nelle rigenerazioni urbanistiche e consolidare la resilienza dei sistemi urbani rispetto al rischio delle alluvioni localizzate.

Sicurezza delle infrastrutture di trasporto

Tra le infrastrutture critiche, una particolare attenzione va rivolta alle reti stradali e ferroviarie nazionali in quanto sistemi nei quali i concetti di robustezza e ridondanza possono non essere economicamente sostenibili e per i quali l'interruzione di servizio di un singolo segmento può mettere a rischio interi corridoi nazionali e transnazionali per il trasporto di persone e merci. Nel nostro Paese, in particolare, esiste una fragilità sistematica delle opere d'arte stradali e, in alcuni casi, di quelle ferroviarie dovute alla naturale obsolescenza di un sistema che si è espanso essenzialmente negli anni '60 e '70 del secolo scorso e che, in questi anni, si sta approssimando alla fine della vita utile di esercizio. L'elevatissimo numero di singole infrastrutture che necessiteranno a brevissimo di interventi di "revamping" o di

sostituzione, misurabile in molte decine di migliaia, rende estremamente problematico coniugare l'urgenza degli interventi con la capacità del Paese in termini di risorse economiche e tecniche, e con le esigenze di garantire il servizio. Appare, quindi, rilevante introdurre dei modelli analitici, sperimentali e tecnologici che possano aiutare a definire le priorità degli interventi e l'uso razionale delle risorse disponibili. Sotto questo profilo, quindi, appare necessario uno sforzo di ricerca che modifichi l'attuale paradigma in termini di monitoraggio delle opere d'arte stradali e ferroviarie, in particolare dei ponti, trasformandolo da intervento di conoscenza su un singolo item ad un sistema globale che permetta di seguire l'evoluzione contemporanea di moltissimi segmenti delle reti di trasporto interpretandone, per quanto possibile, le mutue interazioni anche in riferimento al traffico veicolare e ferroviario. Anche in questi casi appare indispensabile che la ricerca proponga tecniche e tecnologie, basate su una sempre più ampia ed efficace diffusione di robotica, *big data* e *digital twin,* da applicare alle infrastrutture a servizio delle reti stradali e ferroviarie, in particolare con analisi dei *big data* di monitoraggio (anche traendo beneficio dagli sviluppo dell'intelligenza artificiale e del machine learning) finalizzata a consentire la rilevazione e previsione dell'evoluzione di degradi e comportamenti anomali, ai fini del loro controllo mediante manutenzione su condizione e predittiva. Inoltre, attesa la completa esposizione all'aperto ed il numero molto elevato di infrastrutture da monitorare, appare inevitabile contestualizzare anche al tema specifico le tecniche di osservazione basate sull'interferometria radar satellitare, al momento sviluppate solo a livello concettuale nei riguardi delle infrastrutture di trasporto.

Impatti

Con riferimento a quanto previsto nel Programma Horizon Europe 21-27, gli impatti principali sono riconducibili a:

- *"Resilience and autonomy of physical and digital infrastructures are enhanced and vital societal functions are ensured with the help of modern technologies, as well as better cooperation between stakeholders",* con particolare riferimento allo statement associato *"Improved security and resilience of infrastructure and vital societal functions"*
- *"Losses from natural, accidental and man-made disasters are reduced through better societal resilience and improved disaster risk management",* con particolare riferimento allo statement associato *"Improved disaster risk management and societal resilience".*

Più in particolare, in relazione agli obiettivi individuati, va osservato che gli edifici storici, siti archeologici e monumenti rappresentano una parte fondamentale del patrimonio culturale e dell'identità stessa dell'Italia che possono beneficiare delle metodologie e tecnologie di monitoraggio e prevenzione dei rischi.

Altro impatto positivo che l'attività di ricerca proposta può garantire consiste nel miglioramento delle condizioni di sicurezza e resilienza del Paese e delle infrastrutture critiche in presenza di eventi eccezionali come i rapidi mutamenti climatici, i disastri naturali, attacchi intenzionali fisici e cyber, eventi inattesi come ad es. la crisi sanitaria Covid-19, e i mutamenti tecnologici e di mercato di alcuni settori in rapida evoluzione.

Un impatto rilevante dell'attività di ricerca, evidenziata in alcuni obiettivi legati alle infrastrutture energetiche, è rappresentato dalla possibilità di ottemperare a quanto prospettato nel Piano nazionale energia e clima 2030 (PNIEC 2030) e richiesto dagli obiettivi europei in tema di decarbonizzazione e utilizzo delle fonti rinnovabili senza pregiudicare la Security e la Resilienza delle infrastrutture energetiche. Le ricadute di tali attività di ricerca sono sicuramente di interesse per la comunità, oltre che per il sistema industriale italiano e delle PMI (costruttrici di componenti e apparati). Di rilievo anche le ricadute sul sistema di standardizzazione internazionale (CIGRE, IEC e CENELEC) e nazionale (CEI) nonché sugli aspetti regolatori e istituzionali in tema di energia.

Nell'ambito delle infrastrutture idrauliche, l'attività di ricerca condurrà alla riduzione delle perdite nelle reti acquedottistiche, oggi molto elevate, alla definizione delle priorità di intervento di riqualificazione delle reti ed alla razionalizzazione del sistema di monitoraggio e misura.

Infine, incrementare la sicurezza e la resilienza delle infrastrutture critiche grazie a servizi di monitoraggio e comunicazione satellitare può produrre applicazioni che vanno ad espandere il settore dell'aerospazio e dell'industria elettronica ed elettrotecnica italiana. La possibilità di servire anche di più di una infrastruttura con uno stesso sistema di monitoraggio e comunicazione può dare origine a utili economie di scala e l'interesse di grandi *player* industriali

nel settore delle *utility* può creare un effetto leva sui finanziamenti alla ricerca in questo comparto industriale. L'effetto finale è potenziare la filiera italiana dell'aerospazio, delle apparecchiature elettroniche e l'industria elettrica.

Interconnessione con altri ambiti tematici

Sulla base di quanto evidenziato appaiono evidenti forti interconnessioni di questo Ambito tematico e di questa articolazione in particolare con una serie di altre articolazioni proprio in virtù del carattere ampio e interdisciplinare del settore della Sicurezza e Resilienza, per la numerosità delle strutture, infrastrutture e reti che possono beneficiare dei risultati della ricerca e del necessario riferimento agli aspetti tecnologici specifici che caratterizzano li sistemi di monitoraggio, controllo e prevenzione dei rischi.

- **Patrimonio Culturale:** i sistemi di monitoraggio svolgono un ruolo fondamentale nella salvaguardia del valore inestimabile dei beni culturali, architettonici e ambientali del nostro Paese. Pertanto, la riqualificazione strutturale e la rigenerazione necessaria per migliorare la sicurezza richiede un approccio multidisciplinare che coinvolge esperti di varie estrazioni culturali.
- **Sicurezza Sistemi Naturali:** in questo ambito tematico l'attenzione si focalizza sui sistemi di monitoraggio e prevenzione di eventi naturali estremi (frane, alluvioni, ondate di calore) per cui lo sviluppo di strumenti di previsione risulta importante per l'incremento della resilienza o di eventi fortemente impattanti, quali i terremoti, sui quali si è sviluppata una accresciuta sensibilità che mira ad un più alto livello di protezione delle strutture e delle infrastrutture critiche.
- **Cambiamenti Climatici e Adattamento:** in questo ambito tematico e in molti programmi di ricerca europei si pone l'accento sulla sicurezza delle infrastrutture critiche e sull'utilizzo delle risorse idriche e naturali per migliorare la sicurezza della catena agroalimentare. Questa articolazione può avvantaggiarsi di un lavoro coordinato con l'ambito tematico sui cambiamenti climatici poiché i sistemi di monitoraggio sviluppati nell'ambito della sicurezza e resilienza possono basarsi su metodologie di previsione, sistemi e tecnologie sviluppate in questo ambito. Viceversa, esiste una importante attività di ricerca europea e nazionale (ad esempio nell'ambito della cosiddetta Ricerca di Sistema) sviluppata per la protezione delle infrastrutture critiche che può mettere a disposizione strumenti, metodologie e software che possono essere utilizzate in studi e ricerche nell'ambito dei cambiamenti climatici. Infine, la necessità di alcune infrastrutture critiche largamente disperse sul territorio (energia, acqua, trasporti, telecomunicazioni etc) di dotarsi di propri sistemi di monitoraggio e previsione del rischio permetterebbe la realizzazione di sistemi integrati che possono essere messi al servizio di alcune filiere quali, ad esempio, quella dell'agro-alimentare; a tale riguardo risultano interessanti alcuni esperimenti di sinergie tra monitoraggio ambientale delle infrastrutture elettriche e settore vinicolo.
- **Energetica industriale:** forte il legame con questo ambito tematico in virtù dell'ampio tema della transizione energetica che, come si è detto, obbliga le infrastrutture energetiche ad una rivisitazione ed allo sviluppo dei sistemi di monitoraggio e controllo per la prevenzione dei rischi a fronte di una rapida evoluzione tecnologica del settore.
- **Aerospazio:** le tematiche di ricerca dell'ambito tematico Aerospazio possono essere sicuramente di interesse per questa articolazione che si potrà avvalere degli avanzamenti tecnologici del settore ampliando, d'altro canto, il settore delle applicazioni di interesse per questa filiera produttiva (si veda ad esempio quanto detto a proposito della costellazione GALILEO e dell'uso di satelliti a basso costo).
- **Cybersecurity:** ambito tematico all'interno dello stesso Ambito di riferimento per questa articolazione. È evidente il legame stretto con le problematiche della Sicurezza e dei sistemi di monitoraggio e controllo delle infrastrutture critiche. L'interconnessione dei due tavoli tematici appare naturale visto il doppio aspetto della sicurezza fisica e cyber con risvolti che sono fortemente interdipendenti. È possibile poi che possano esserci interconnessioni con attività di ricerca e sviluppo per le attività del Ministero degli Interni e della Difesa. Infatti, la protezione delle infrastrutture critiche nei confronti di attacchi terroristici e sabotaggio sia fisico che cyber è un tema rilevante che richiede un collegamento ed un'attività di coordinamento anche con altre Istituzioni preposte alla difesa di infrastrutture (elettricità, gas, acqua, trasporti, mercati correlati) essenziali per la convivenza civile e la sopravvivenza dello Stato. Non a caso un caposaldo nella nascita dell'interesse verso le Infrastrutture critiche è dato dal US Presidential Decision Directive PDD-63 di Bill Clinton nel 1998 in cui si

sostiene la rilevanza strategica della protezione di "those physical and cyber-based systems essential to the minimum operations of the economy and government ".

Key Performance Indicators

La qualità dei risultati della ricerca e degli impatti raggiunti potrà essere valutata mediante specifici indicatori, tra i quali:

Impatto scientifico

- bibliometria delle pubblicazioni scientifiche (misura del numero e dell'impatto)
- brevetti assegnati
- borse di studio di dottorato
- altre iniziative di alta formazione
- Numero, impatto e finanziamenti per nuova ricerca interdisciplinare e nuove filiere della conoscenza
- Numerosità ed entità degli organismi di ricerca italiani coinvolti
- Numerosità dei rapporti e qualità del coordinamento con altri programmi di finanziamento (ad es., Programmi europei, Ricerca di Sistema etc.)
- Replicabilità ed utilizzabilità dei risultati su più filiere
- Diffusione dei risultati (articoli, siti web, eventi, conferenze, attività di standardizzazione)

Impatto industriale

- finanziamenti acquisiti
- iniziative d'impresa
- partenariati pubblico-privati
- impiego dei ricercatori coinvolti nelle attività di ricerca e sviluppo di imprese
- borse di studio di dottorato industriale
- progressiva sensibilizzazione e attivazione dei grandi player industriali per mantenere e accrescere il presidio nazionale in settori strategici.
- numerosità delle filiere produttive e tipologie di *utility* interessate

Impatto pubblico

- implementazione dei risultati nelle pubbliche amministrazioni
- ottimizzazione dei costi della sicurezza e della resilienza nella pianificazione e gestione delle infrastrutture
- impiego dei ricercatori coinvolti nelle attività degli enti pubblici di gestione delle infrastrutture
- numero di prodotti di ricerca utili per le attività regolatorie

Impatto economico

- indicatori della Strategia Energetica Nazionale SEN 2017 del MiSE e MATTM (2017)
- indicatori del Piano nazionale energia e clima 2030 (PNIEC 2030) del MiSE (2020)
- riduzione delle perdite relative ai rischi in esame
- ottimizzazione delle risorse per la gestione della sicurezza
- riduzione degli effetti dei rischi correlati a infrastrutture critiche sui mercati connessi
- effetti sulla bilancia dei pagamenti della tecnologia

Impatto sulle questioni ambientali

- indicatori della Strategia Nazionale per lo Sviluppo Sostenibile del MATTM (2017) e definiti dall'ISTAT (2020) in relazione al raggiungimento dei 17 SDGs dell'Agenda 2030.
- indicatori della Strategia Energetica Nazionale SEN 2017 del MiSE e MATTM (2017)
- indicatori del Piano nazionale energia e clima 2030 (PNIEC 2030) del MiSE (2020)

Impatto sulla sicurezza del cittadino

- riduzione rischi dovuti a perdite di servizi essenziali
- riduzione rischi dovuti a effetti a cascata indotti da perdite di infrastrutture critiche su mercati, mercato del lavoro, disagio del vivere civile, etc.

Articolazione 3. Gestione dei rischi e della resilienza

La continuità della vita delle comunità è assicurata da una serie di infrastrutture civili che garantiscono la produzione, distribuzione e fruizione di beni materiali e di servizi. Tali sistemi sono fortemente interconnessi a causa di legami fisici e logico-funzionali tali da costituire un complesso sistema di sistemi. In questa logica, questo sistema è il cosiddetto ambiente costruito e, nella letteratura tecnica relativa, si può modellare logicamente come una serie di strati sovrapposti in cui, di solito, lo strato più superficiale è rappresentato dalle attività che hanno luogo negli edifici e nelle strutture in genere, mentre strati inferiori sono le reti di utilità. Questo schema logico è rappresentato in Figura 1.

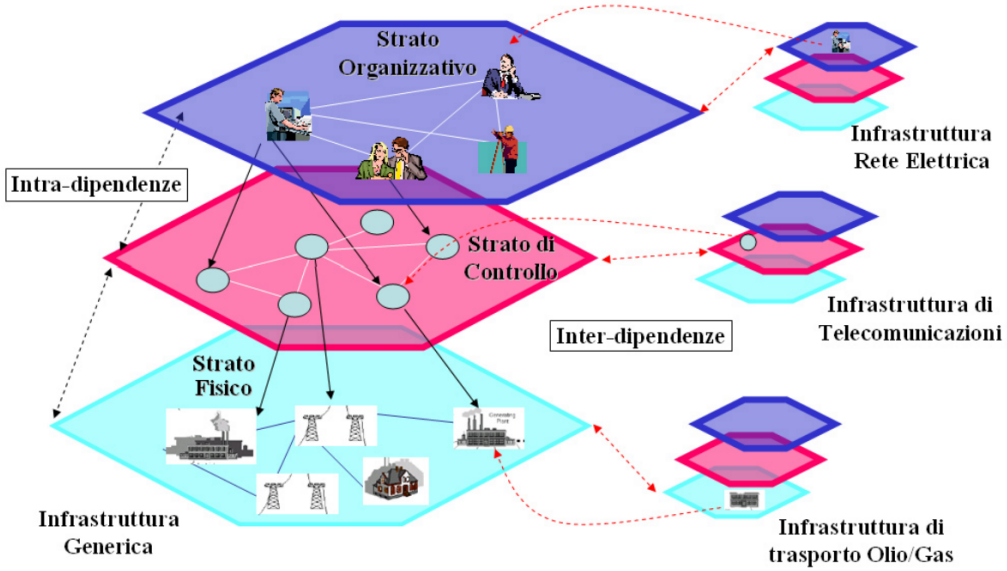

Figura 1. Ambiente costruito come sistema complesso di infrastrutture interdipendenti.[1]

Le scale di sviluppo della rappresentazione riportata in Figura 1 sono molteplici. Dal punto di vista spaziale, la scala più di dettaglio è quella della singola struttura, rete o infrastruttura, per passare poi al sistema di infrastrutture alla scala urbana, regionale, nazionale o anche sovra-nazionale. A questo proposito, sono incluse in questo schema anche le reti di approvvigionamento di beni e servizi e semi-lavorati. La *sicurezza* quindi dipende dalla reazione a *cause di disturbo* (eventi calamitosi, naturali o antropici) della funzionalità delle infrastrutture che costituiscono l'ambiente costruito e il riflesso sulle comunità, e più in generale su portatori di interesse serviti.

L'andamento nel tempo della funzionalità dopo una perturbazione ha a che fare con la *resilienza* del sistema e/o della comunità servita.

In termini quantitativi, la resilienza può essere definita in relazione al processo di recupero della qualità (funzionalità) di un sistema perturbato da un evento dannoso, di natura naturale o antropica. La valutazione dell'entità della perdita di funzionalità del sistema è oggetto della analisi di rischio. Il recupero da tale perdita, per il ripristino (anche parziale o più che totale) della funzionalità, riguarda la resilienza, che viene tipicamente caratterizzata dalla robustezza del sistema (i.e., la capacità del sistema di sopportare la perturbazione derivante dall'evento dannoso, mitigandone gli

[1] Da https://didattica-2000.archived.uniroma2.it//GovernoDigitale/deposito/Infrastrutture_critiche.pdf

effetti di perdita di funzionalità), supportata dalla ridondanza funzionale (i.e., la capacità del sistema di continuare a fornire la funzionalità anche avendo subito perdite). La gestione integrata dei rischi cui è esposto il sistema complesso modula gli attributi influendo sul comportamento resiliente dello stesso.

La resilienza è legata ad una serie di azioni di prevenzione, preparazione e pianificazione dell'emergenza (preparedness), risposta alla crisi e recupero di funzionalità e servizio (riconducibili al *Disaster Risk Management cycle* del "*Sendai Framework for Disaster Risk Reduction 2015-2030*" e al nuovo "*Union Civil Protection Mechanism*"). Tali azioni determinano la capacità del sistema di prevenire eventi potenzialmente dannosi, di mitigarne gli effetti, di prepararsi e reagire a tali eventi, infine, di ristabilire la funzionalità e il servizio in tempi accettabili. In particolare, la resilienza per una efficace gestione dei rischi richiede una grande attenzione verso le azioni di prevenzione e *preparedness* che possono incidere in modo rilevante sul livello di prestazione pre-evento, su quello post-evento (perdite) e sui tempi e modalità di recupero.

Nel caso di perturbazione istantanea (es. terremoto), la resilienza si può rappresentare schematicamente come in Figura 2.

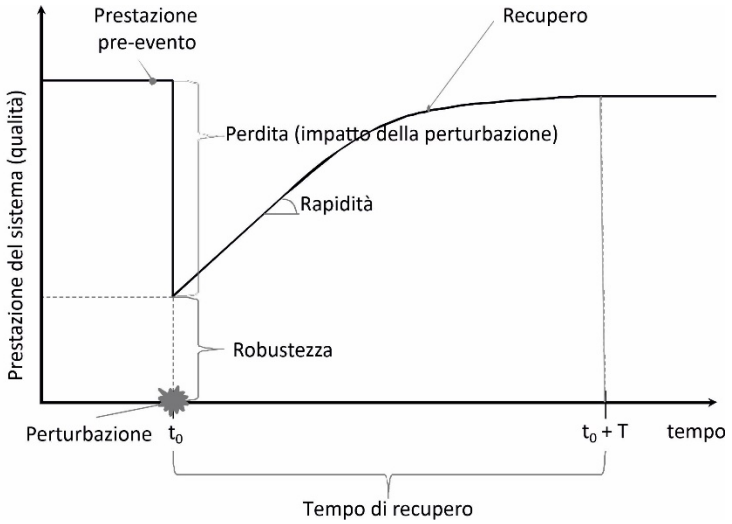

Figura 2. Rappresentazione schematica della resilienza di un sistema e fattori che la determinano.[2]

Nella rappresentazione in Figura 2 la funzionalità rappresenta genericamente un parametro di qualità della prestazione del sistema, incluso gli effetti diretti sui cittadini parte delle comunità servite. Una rappresentazione simile è possibile anche nel caso di eventi i cui effetti non siano istantanei. Ciò può avvenire sia per la natura stessa della perturbazione sia per la capacità del sistema di reagire rapidamente durante l'evoluzione stessa del disturbo cercando di minimizzare la perdita di prestazioni. In questo caso, l'infrastruttura tenta di assorbire l'impatto di un tale evento minimizzando la perdita di funzionalità e cercando di garantire le condizioni per un rapido recupero (*restoration*) delle condizioni normali di funzionamento. È necessario, quindi, garantire al meglio la capacità di sopravvivenza (*survivability*) e di autoriparazione (*self-healing*) del sistema. Alcune infrastrutture critiche caratterizzate da una capacità di reazione sufficientemente veloce possono operare efficaci azioni di controllo in emergenza e in ripristino. Per queste tipologie di infrastrutture, la ricerca dei prossimi anni deve, quindi, individuare i componenti, le tecnologie e le strategie di controllo in grado di adottare i sistemi della necessaria flessibilità e rapidità di azione per adattarsi a cambiamenti repentini, senza deprimere eccessivamente le proprie prestazioni a fronte di vulnerabilità che possono essere fisiche, cyber e cyber-fisiche.

È anche necessario considerare che gli eventi possono essere multipli e ravvicinati, quando il recupero è già iniziato. In questo senso, bisogna prevedere che il processo di recupero possa non essere monotono nel tempo.

[2] Da https://open.library.ubc.ca/cIRcle/collections/53032/items/1.0076088

Dalla Figura 2, si osserva come le perdite causate dall'evento perturbativo determinino il punto di partenza della fase di recupero. L'analisi di rischio si occupa della valutazione di tali possibili perdite dovute alla realizzazione di potenziali pericoli individuati e, in tal senso, l'analisi di resilienza include l'analisi di rischio, ma richiede anche l'analisi di robustezza al fine di valutare la parte di funzionalità che il sistema è in grado di mantenere a seguito della perturbazione. L'analisi di resilienza si estende, infine, alla valutazione degli attributi del sistema che ne determinano il recupero della funzionalità. Ad esempio, la rapidità di recupero ha a che fare con la disponibilità e la gestione delle risorse per il recupero. Data la dimensione temporale della resilienza, è necessario distinguere la scala a cui operano i sistemi oggetto di analisi, e dal punto di vista della gestione degli eventi, naturali e antropici, che possono determinare la perturbazione, è d'uso distinguere il breve termine dopo l'evento (gestione delle emergenze), il medio termine in cui la comunità recupera una certa funzionalità di regime, e il lungo termine che ha a che fare con il ciclo di vita delle infrastrutture.

La capacità di assorbire i disturbi e garantire il ripristino più rapido possibile delle condizioni normali di funzionamento dipende dalla capacità di pianificare le linee di difesa (*preparedness*) e i sistemi di controllo e di gestione idonei ad operare in condizioni di emergenza. Un'accurata progettazione che consideri sin dall'inizio i fenomeni ad alto impatto e bassa frequenza, la capacità del sistema di riconoscere i fenomeni in corso e di riorganizzarsi, la disponibilità di componenti e tecnologie idonee al controllo delle condizioni di funzionamento fortemente perturbate, la disponibilità di strategie di controllo e protezione che minimizzino la perdita delle prestazioni, la pianificazione sequenziale dinamica delle fasi di ripristino a fronte degli scenari di incidente, sono tutti elementi fondamentali per garantire la resilienza del sistema e per questo devono essere oggetto di studi approfonditi nei prossimi anni.

Obiettivi

In tale articolazione rientrano una serie di settori, di necessità fortemente interdisciplinari, nei quali sviluppare conoscenze, competenze e tecnologie per la sicurezza dell'ambiente fisico ai fini della gestione dei rischi e della resilienza dei sistemi e delle comunità che li vivono. Ciò include i metodi di cui all'Articolazione 1, finalizzati alla conoscenza e analisi dei rischi attraverso la modellazione sistemica e l'approfondimento delle caratteristiche dei sistemi in riferimento alle componenti del rischio e alle interdipendenze che li caratterizzano.

Nella valutazione dei rischi cui è soggetto l'ambiente costruito, finalizzata alla loro gestione, rivestono un ruolo primario la modellazione, analisi e monitoraggio delle **perdite** per i diversi componenti del sistema fisico, in conseguenza dell'impatto delle cause di perturbazione descritte in precedenza. Si parla in generale di caratterizzazione e controllo della *vulnerabilità* dell'ambiente costruito, intesa come propensione a subire perdite sotto l'azione delle suddette cause di perturbazione, considerando anche gli eventi concomitanti e gli effetti a cascata. A tal fine devono essere quindi elaborate e proposte azioni per la mitigazione e gestione dei rischi specificamente riferite ai diversi tipi di pericoli considerati e per le diverse componenti del sistema, sia quelle fisiche sia – e in maniera non secondaria – quelle funzionali e quelle economiche. Tra le componenti vulnerabili vanno annoverate sia quelle singole (quali ad esempio singoli edifici o singoli componenti facenti parti di infrastrutture distribuite) che le classi (o gruppi) costituite dall'unione di più componenti, e in maniera specifica le lifelines, ovvero infrastrutture che forniscono servizi vitali e che sono caratterizzate sia da interconnessioni tra i vari sottosistemi che le compongono che da intra-connessioni tra i vari componenti che formano il singolo sottosistema. In questi casi, devono essere definiti dei modelli di analisi della vulnerabilità in grado di tener conto anche di tali connessioni.

Un ulteriore aspetto di rilievo sono le tecnologie atte alla caratterizzazione dell'ambiente costruito, che spesso è conosciuto in modo molto parziale, tale per cui non è possibile applicare efficacemente le tecnologie per l'analisi e la gestione dei rischi e della resilienza. In questo ambito si può parlare di tecnologie per la caratterizzazione dell'*esposizione*. Si intende, con questo termine, lo sviluppo di strumenti e tecnologie per la definizione di modelli che descrivono l'ambiente costruito atti alla analisi dei rischi e della resilienza. Anche i sistemi di monitoraggio della funzionalità e la qualità delle prestazioni delle infrastrutture sono da considerarsi pertinenti.

Nella gestione dei rischi, la prevenzione può essere perseguita adottando tre possibili strategie:

S1. adozione diffusa di efficaci norme di progettazione (*Building Better from the Start*, BBS);

S2. programmi di rafforzamento post-evento che migliorino le prestazioni di strutture ed infrastrutture rispetto alla condizione ante-evento (*Build Back Better*, BBB);

S3. programmi di riabilitazione in territori con livelli elevati di rischio (ossia intervenendo prima e non dopo per riparare danni e rafforzare gli elementi colpiti).

Per decidere quale strategia perseguire e, soprattutto, come esse vadano opportunamente combinate per una ottimale allocazione delle risorse, sono necessari studi e ricerche che operino con approccio olistico e interdisciplinare in un contesto multi-rischio.

Con riferimento alla strategia S1 è necessario produrre codici normativi per le strutture e le infrastrutture di nuova generazione che superino i limiti che emergono nella applicazione di quelli correnti. Ad esempio, l'attuale approccio alla progettazione strutturale non sempre garantisce uniformità del rischio tra costruzioni dello stesso tipo in siti a pericolosità diversa e tra tipologie strutturali diverse progettate nello stesso sito, pertanto vanno riviste le filosofie alla base della definizione e gestione del rischio.

Per quanto riguarda specificamente la mitigazione del rischio sismico, ma in qualche modo in analogia ad altri rischi naturali, un aspetto cruciale, sia nell'azione BBB (strategia S2) che nella riabilitazione pre-evento (strategia S3), è decidere sul tipo di intervento, ossia decidere tra recupero e sostituzione edilizia. In Paesi come l'Italia, con i suoi centri storici e la grande diffusione di costruzioni storiche o monumentali, la scelta è frequentemente quella del recupero, e ciò richiede ricerche per l'ulteriore sviluppo di soluzioni di intervento non invasive e sostenibili sul piano dei costi e dell'impatto. Nel caso di costruzioni ordinarie progettate secondo codici obsoleti, talvolta realizzate con materiali di scarsa qualità, e giunte in molti casi al termine della propria vita utile, l'elevata vulnerabilità, ampiamente testimoniata da recenti eventi sismici, suggerisce interventi di sostituzione edilizia.

Infine, a valle di eventi calamitosi particolarmente gravi, nella applicazione della strategia S2 appare importante definire anche criteri che indirizzino le scelte alla scala urbanistica e non di singoli manufatti. È importante sviluppare attività di ricerca (modelli previsionali, analisi geologiche, studi sociali e storici, analisi costi-benefici) che consentano di valutare l'opportunità sociale, economica e tecnica di spostare in altro luogo comunità che hanno subito eventi distruttivi, in particolare nel caso di elevata probabilità di ripetizione a breve-medio termine di tali eventi che, unita a sfavorevoli caratteristiche geologiche ed orografiche, potrebbe suggerire di trasferire in altri luoghi interi agglomerati urbani.

Per quanto riguarda il rischio idrogeologico, è necessario un avanzamento delle capacità di previsione degli eventi e dei loro impatti, a tutte le scale geografiche e temporali, nel contesto dei cambiamenti climatici e ambientali in atto o previsti. In tal senso, va migliorato e reso più efficace ciò che è stato introdotto con la Legge 183 del 1989, in particolare omogeneizzando e ammodernando i Piani di Assetto Idrogeologico e i Piani di Gestione del Rischio di Alluvioni. Tale obiettivo va raggiunto con attività sinergiche che producano avanzamenti nelle capacità di: (i) riconoscere, individuare e cartografare le frane e le aree inondate, dalla scala locale a quella globale; (ii) sviluppare sistemi previsionali, e in particolare sistemi "operativi" che consentano una risposta rapida al possibile verificarsi di eventi di frana locali, colate di detrito e piene improvvise; (iii) sviluppare proiezioni della franosità e del rischio alluvionale in risposta ai cambiamenti climatici e ambientali in atto e attesi; (iv) produrre modelli previsionali del rischio geologico, geomorfologico e idraulico, con attenzione al rischio per la popolazione; (v) fornire soluzioni per interventi di mitigazione attraverso la riprogettazione del paesaggio rurale e urbano, e l'introduzione di prescrizioni urbanistiche e tecniche costruttive che riducano la vulnerabilità degli edifici e delle persone.

Impatti

Per le attività di ricerca da sviluppare nel campo della Gestione dei Rischi e della Resilienza si prevedono i seguenti impatti principali:

- Sviluppo di conoscenze, competenze e tecnologie relative agli attributi della resilienza dell'ambiente fisico per la *lifeline* delle comunità a scala urbana, regionale, nazionale o sovranazionale.
- Selezione, definizione e realizzazione dinamica di strategie per la riduzione delle perdite e il miglioramento della resilienza di infrastrutture e reti, e in ultima analisi della sicurezza dell'ambiente costruito.

- Sviluppo di modelli per la valutazione delle strategie ottimali dal punto di vista della allocazione delle risorse, anche in termini benefici/costi.
- Definizione di strategie dinamiche ottimizzate per la riduzione delle perdite e del decadimento delle prestazioni in condizioni di emergenza.
- Sviluppo di sistemi avanzati di controllo della resilienza di infrastrutture critiche e reti.
- Programmi di riabilitazione preventiva e di preparazione ai disastri in territori con livelli elevati di rischio. A tale scopo, sono necessari studi e ricerche che consentano di stabilire criteri e metodi per la individuazione della strategia ottimale, con un approccio olistico e interdisciplinare nel contesto multi-rischio e multi-hazard.
- Strumenti di supporto alle decisioni per la gestione delle risorse destinate a politiche di mitigazione e per le scelte relative all'allocazione delle risorse, in base a criteri di prioritizzazione relativi ai diversi componenti dell'ambiente costruito.

Interconnessioni

Le interconnessioni dell'ambiente costruito possono riguardare diversi Grandi Ambiti di ricerca ed Ambiti Tematici, in particolare:

- Ambito CLIMA, ENERGIA MOBILITÀ SOSTENIBILE
  a. CAMBIAMENTI CLIMATICI E ADATTAMENTO, per quanto riguarda i rischi naturali che minacciano le infrastrutture;
  b. MOBILITÀ SOSTENIBILE, nella misura in cui il sistema di trasporto rappresenta uno dei componenti dell'ambiente costruito;
- Ambito CULTURA UMANISTICA, CREATIVITÀ, TRASFORMAZIONI SOCIALI, SOCIETÀ DELL'INCLUSIONE
  c. PATRIMONIO CULTURALE, per quanto riguarda il patrimonio artistico e monumentale come una componente infrastrutturale dell'ambiente costruito;
  d. TRANSFORMAZIONI SOCIALI, SOCIETÀ DELL'INCLUSIONE, per quanto riguarda la preparazione alla convivenza con i rischi e la cultura della sicurezza e della prevenzione;
- Ambito INFORMATICA, INDUSTRIA, AEREOSPAZIO
  e. HIGH PERFORMING COMPUTING per l'analisi e la gestione delle informazioni relative alla gestione della sicurezza e della resilienza di sistemi infrastrutturali complessi;
  f. INTELLIGENZA ARTIFICIALE, per l'analisi della sicurezza di sistemi complessi e per il monitoraggio continuo e automatico dei rischi;
  g. ROBOTICA, per il monitoraggio continuo e automatico dei pericoli e dei rischi cui è sottoposto l'ambiente costruito, ed in particolare le infrastrutture critiche, nonché per il supporto alle attività di pianificazione (preparedness) e di gestione dell'emergenza, in particolare in ambiente ostile (es. ruolo dei cosiddetti "first responders").

Per quanto riguarda l'ambito di ricerca SICUREZZA PER I SISTEMI SOCIALI, vi è una particolare connessione con l'ambito tematico SICUREZZA SISTEMI NATURALI, perché tali sistemi sono anch'essi sistemi complessi collegati e interdipendenti con l'ambiente costruito. Inoltre, anche la connessione con l'ambito CYBERSECURITY è rilevante avendo a che fare con un rischio antropico potenzialmente importante per una serie di infrastrutture strategiche, come il sistema bancario e tutte le infrastrutture governate attraverso sistemi informatici (es. infrastrutture di trasporto).

Key performance indicators

La qualità dei risultati della ricerca e degli impatti raggiunti potrà essere valutata mediante specifici indicatori, tra i quali:

- Eccellenza scientifica
  - bibliometria delle pubblicazioni scientifiche (misura del numero e dell'impatto)
  - brevetti assegnati
  - borse di studio di dottorato

  - altre iniziative di alta formazione
- Impatto industriale
  - finanziamenti acquisiti
  - iniziative d'impresa
  - partenariati pubblico-privati
  - impiego dei ricercatori coinvolti nelle attività di ricerca e sviluppo di imprese
  - borse di studio di dottorato industriale
- Impatto pubblico
  - implementazione dei risultati nelle pubbliche amministrazioni
  - ottimizzazione dei costi di gestione delle infrastrutture
  - impiego dei ricercatori coinvolti nelle attività degli enti pubblici di gestione e operazione delle infrastrutture
- Impatto economico
  - riduzione delle perdite relative ai rischi in esame
  - ottimizzazione delle risorse per la gestione della sicurezza
  - riduzione dei costi di manutenzione per la gestione delle infrastrutture
- Impatto sulla sicurezza del cittadino
  - omogeneizzazione dei rischi cui è esposto il cittadino durante la vita nell'ambiente costruito per i rischi in esame
  - consapevolezza dei rischi e preparazione a eventi calamitosi

Articolazione 4. Sicurezza e resilienza per la società e lo sviluppo sostenibile

La sicurezza e la resilienza delle strutture, infrastrutture e reti che forniscono servizi essenziali per il funzionamento della nostra società, sono elementi fondanti per il suo sviluppo sostenibile. Per questo, va sempre più favorito il coinvolgimento della società civile su questi temi e sulla loro evoluzione a fronte della continua e rapida innovazione tecnologica e dei cambiamenti ambientali e sociali. Questa attenzione al coinvolgimento dei cittadini era già presente nel programma '*Science with and for Society*' e nella sfida sociale "*Secure Societies – protecting freedom and security of Europe and its citizens*" del Programma Horizon 2020. Tuttavia, per contribuire allo sviluppo sostenibile dei territori e delle comunità, vanno ancor più rafforzati l'informazione, la consapevolezza, la preparazione ed i comportamenti attivi dei cittadini nel gestire la sicurezza e la resilienza delle persone e dei beni materiali rispetto ai rischi naturali ed antropici.

D'altra parte, la ratifica dell'Accordo di Parigi sul Clima, sostenuto in modo convinto dai Paesi europei, Italia compresa, nasce dalla sensibilità maturata nella società civile sull'urgenza di azioni di mitigazione del riscaldamento globale e di capacità di adattamento ai suoi impatti sui sistemi e sull'ambiente costruito. Questo ha contribuito a delineare la politica del Green Deal europeo che si tradurrà in azioni di stimolo per attività di ricerca e innovazione che hanno proprio nello sviluppo sostenibile il comune denominatore.

Coerentemente, nel Programma Horizon Europe 2021-27 è previsto il Cluster 3 "*Civil Security for Society*" (ved. documento "*Orientations towards the first Strategic Plan for Horizon Europe*", dicembre 2019). Il Cluster 3 affronta temi attinenti alla sicurezza delle strutture, infrastrutture e reti, evidenziando priorità di ricerca che, considerando specificamente gli aspetti della sicurezza e resilienza previsti nell'Ambito Tematico 3.1, riguardano soprattutto i rischi legati al clima e relativi eventi estremi (incendi, siccità, alluvioni, ondate di calore e tempeste, etc.) ed a catastrofi geologiche, in particolare i terremoti.

Riferimento importante, nel contesto italiano, è anche il nuovo Codice di Protezione Civile (2018), nel quale si precisa che: "*La prevenzione consiste nell'insieme delle attività di natura strutturale e non strutturale, svolte anche in forma integrata, dirette a evitare o a ridurre la possibilità che si verifichino danni conseguenti a eventi calamitosi anche sulla base delle conoscenze acquisite per effetto delle attività di previsione.*" I temi trattati in questa articolazione si inseriscono specificamente all'interno della "prevenzione non strutturale" per la quale il Codice, tra le diverse azioni, prevede attività relative a:

(i) *la diffusione della conoscenza e della cultura della protezione civile, anche con il coinvolgimento delle istituzioni scolastiche, allo scopo di promuovere la resilienza delle comunità e l'adozione di comportamenti consapevoli e misure di autoprotezione da parte dei cittadini;*
(ii) *l'informazione alla popolazione sugli scenari di rischio e le relative norme di comportamento nonché' sulla pianificazione di protezione civile;*
(iii) *la promozione e l'organizzazione di esercitazioni ed altre attività addestrative e formative, anche con il coinvolgimento delle comunità, sul territorio nazionale al fine di promuovere l'esercizio integrato e partecipato della funzione di protezione civile.*

La dimensione sociale della sicurezza e della resilienza riguarda la dinamica della comunicazione e percezione del rischio nel coinvolgimento di attori assai diversi, quali scienziati, esperti, decisori e cittadini comuni. Opportuni filoni di ricerca andranno promossi a cavallo tra 'scienze dure', scienze sociali, economiche e umane per sviluppare e consolidare una percezione condivisa da parte della società tutta sulla sicurezza e resilienza di strutture, infrastrutture e reti, e sul rischio residuo socialmente accettabile, in base ad analisi costi-benefici sociali che permettano di identificare le priorità di intervento per lo sviluppo sostenibile delle comunità, in funzione delle risorse disponibili.

Gli obiettivi ineludibili di riduzione delle emissioni climalteranti spingono verso una rapida ristrutturazione e riorganizzazione di alcune infrastrutture creando nuove opportunità di sviluppo ma anche nuove problematiche in termini di sicurezza e resilienza.

Un esempio rilevante è il passaggio rapido da un sistema energetico centralizzato ad uno decentralizzato risultante dalla transizione energetica da fonti di energia prevalentemente fossili a fonti rinnovabili. In tale contesto, principale obiettivo delle ricerche dovrà essere la definizione di soluzioni in grado di coniugare le forti istanze sociali e la propensione sviluppatasi verso l'uso di fonti rinnovabili con l'esigenza di una gestione sicura e resiliente delle infrastrutture, su orizzonti temporali di lungo termine. Pertanto, nel PNR 2021-27 andrà sostenuta la ricerca per lo sviluppo delle varie forme di accumulo (elettrochimico, idroelettrico/pompaggio anche di piccola taglia, Power to Gas, P2X etc.), di tecnologie per garantire la flessibilità del sistema e metodologie per il controllo e gestione della sicurezza. La reinterpretazione dell'infrastruttura elettrica vista in chiave di livelli sempre più spinti di sostenibilità, dovrà tenere conto della sensibilizzazione dei cittadini sui temi dell'utilizzo intelligente dell'energia, diffondendo lo sviluppo delle cosiddette 'smart grids' grazie al sostegno di Intelligenza Artificiale, Cloud Computing, e nuovi standard di comunicazione che permettano una loro gestione *user friendly* ed efficace. La produzione diffusa di energia elettrica e la diffusione di mezzi di trasporto alimentati da energia elettrica e sistemi ibridi, previsti in crescita nei prossimi anni, rende necessaria la ricerca sulla sicurezza dei sistemi di distribuzione dell'energia ai livelli gerarchicamente più bassi poiché costruiti in passato con la logica *fit and forget*. La diffusione della mobilità elettrica costituisce, al tempo stesso, una opportunità per il miglioramento del vivere civile oltre che per la riduzione delle emissioni locali, anche per la possibilità di utilizzare il paradigma V2X che nelle sue varie declinazioni permette di incrementare la sicurezza di distribuzione elettrica (Vehicle to Grid-V2G), delle unità abitative (Vehicle to Home-V2H), del traffico stradale (Vehicle to Vehicle V2V o Vehicle to Road V2R), etc.

Un altro chiaro esempio è la sfida posta dall'aumento delle temperature globali che minaccia la sicurezza (nell'accezione anglosassone di 'security') degli approvvigionamenti idrici in alcune regioni del nostro Paese e del Mondo. Questo comporta la necessità di ricerche per un uso più razionale ed efficiente della risorsa idrica (microirrigazione, irrigazione di precisione con il supporto di sistemi di monitoraggio satellitare e da droni) e delle infrastrutture di derivazione, accumulo e trasporto e per la pianificazione degli interventi nelle zone costiere minacciate dall'innalzamento del livello dei mari, già ampiamente osservato e previsto in accelerazione. Il cambiamento globale del clima ha indotto variazioni nel regime delle precipitazioni che hanno esacerbato la pregressa situazione di ineguale distribuzione delle risorse idriche sul territorio, con aree a rischio siccità e aree soggette ad inondazioni e degrado del territorio. La studio e la progettazione di collegamenti idrici tra aree diverse permetterebbe di sfruttare la capacità di invaso dei bacini in modo più razionale, nel rispetto degli usi plurimi della risorsa e di consentire con l'interposizione di stazioni di pompaggio il superamento delle complessità orografiche del territorio assicurando allo stesso tempo la sicurezza delle forniture e la resilienza delle comunità in caso di crisi idriche. Anche in questo contesto, la società deve essere resa più consapevole ed attiva sui processi in atto e i relativi sviluppi.

Una particolare importanza per questo assumono le iniziative legislative, regolatorie e normative che hanno al centro l'utente e, in particolare, la promozione del ruolo attivo del *prosumer* in forma associata, in quanto la responsabilità nella gestione dell'energia e di risorse, come quella idrica o il suolo, comprende in modo specifico anche l'attenzione alla sicurezza e la cura del territorio. Le comunità energetiche permetteranno la promozione di reti locali, gestite localmente e l'applicazione del concetto di *Transactive energy* in ambiente residenziale, per una maggiore indipendenza energetica su base locale al fine di garantire un uso più efficiente dell'energia ma anche un esercizio più sicuro e resiliente delle reti. L'estensione di questi concetti al mondo industriale e al settore dell'agrifood, porta all'integrazione di distretti industriali e agroalimentari con maggiore sicurezza ed efficienza nella gestione degli scambi di energia, materia, risorse, e dunque la realizzazione di ecodistretti a basso impatto ambientale. Lo sviluppo di questi concetti richiede l'avanzamento di strumenti metodologici analitici, e di intelligenza artificiale e machine learning per l'ottimizzazione integrata di energia, materia, impatto ambientale e cicli di produzione, nonché lo sviluppo di nuove tecnologie per garantire la sicurezza di questi sistemi. Con questa visione, il Paese dovrà contribuire allo sviluppo di un nuovo Piano di Azione sull'economia circolare, previsto dalla "Agenda von del Leyen per l'Europa" per fare in modo che l'uso di materiali, componenti, processi per assicurare la sicurezza di strutture e infrastrutture sia sostenibile, nel significato di non danneggiare in modo permanente l'ambiente e nel limitare il consumo di risorse.

Obiettivi

Gli obiettivi che il PNR si pone per il periodo 2021-27 in relazione all'Ambito Tematico 3.1 sono coerenti con alcune delle *missions* di Horizon Europe e alcuni degli obiettivi dell'Agenda ONU 2030. Delle *missions* di Horizon Europe interessano in particolare, in questa sede:

- *adaptation to climate change including societal transformation,*
- *climate-neutral and smart cities.*

Dei diciassette Sustainable Development Goals (SDGs) previsti nell'Agenda ONU 2030, almeno cinque sono pertinenti all'AT 3.1, considerando la loro declinazione adottata anche dal nostro Paese che, in almeno due casi (SDG9 e SDG 11), pone l'accento specificamente sulla resilienza di infrastrutture e comunità (Camera dei Deputati, giugno 2020):

- SDG6 acqua pulita e igiene: garantire a tutti la disponibilità e la gestione sostenibile dell'acqua e delle strutture igienico sanitarie;
- SDG7 energia pulita e accessibile: assicurare a tutti l'accesso a sistemi di energia economici, affidabili, sostenibili e moderni;
- SDG9 imprese, innovazione e infrastrutture: costruire un'infrastruttura resiliente e promuovere l'innovazione ed una industrializzazione equa, responsabile e sostenibile;
- SDG11 città e comunità sostenibili: rendere le città e gli insediamenti umani inclusivi, sicuri, resilienti e sostenibili;
- SDG13 lotta contro il cambiamento climatico: promuovere azioni, a tutti i livelli, per combattere il cambiamento climatico.

A tale riguardo, un importante elemento di riferimento per le scelte dei prossimi anni nel campo della ricerca e innovazione è costituito dal rapporto recentemente pubblicato dall'ISTAT (2020) che analizza lo stato di raggiungimento dei 17 SDGs, disaggregato anche a scala regionale. In particolare, l'analisi evidenzia le aree dove maggiori sono i margini di miglioramento, sui quali si può incidere con attività di ricerca ed innovazione.

Sul SDG6, in Italia la criticità delle risorse idriche ha assunto rilevanza in alcune zone del paese, prevalentemente del Mezzogiorno, particolarmente vulnerabili. L'intera gestione del ciclo delle acque, dal prelievo, all'adduzione, distribuzione e depurazione delle acque reflue, deve essere ottimizzata per ogni tipologia d'uso, civile, industriale, agricolo, zootecnico ed energetico, attraverso investimenti e innovazione tecnologica lungo tutta la filiera, congiuntamente all'educazione e alla sensibilizzazione sul tema.

L'obbiettivo SDG7 di "assicurare l'accesso universale a servizi energetici economici, affidabili, sostenibili e moderni" risulta di particolare rilevanza anche in Italia soprattutto per le positive ricadute che un utilizzo più efficiente e

razionale delle risorse può avere sullo sviluppo economico e sociale, e in termini di sostenibilità energetica e ambientale, rendendo il Paese meno dipendente dall'importazione di fonti fossili, contribuendo alla mitigazione del riscaldamento globale e migliorando, nel complesso, la sicurezza energetica del Paese. Su questo tema specifico assumono una rilevanza particolare, anche per le attività di ricerca, gli Indicatori individuati dalla Strategia Energetica Nazionale SEN 2017 del MiSE e MATTM (2017), e dal più recente Piano nazionale energia e clima 2030 (PNIEC 2030) del MiSE (2020).

Al rafforzamento della funzione di ricerca e sviluppo è specificatamente dedicato il target 9.5 del SDG9, in quanto il progresso scientifico e tecnologico costituisce un importante fattore di crescita economica e produttiva, di sviluppo sociale e di tutela ambientale. L'ISTAT rileva come gli indicatori della rete ferroviaria mostrano la persistenza di un notevole gap infrastrutturale tra le regioni del Settentrione e del Centro rispetto al Mezzogiorno, che continua a disporre di una rete ferroviaria con indicatori di sicurezza, reti a binario doppio o multiplo, sostenibilità ambientale, reti elettrificate e modernità, reti ad alta velocità, più bassi rispetto al resto del Paese.

Il target 11.b dell'Agenda ONU 2030 chiede entro il 2020 l'adozione di piani integrati orientati alla resilienza in linea con il Framework di Sendai per la Riduzione del Rischio di Disastri 2015-2030 e pone al centro della strategia nazionale il miglioramento della qualità ambientale con le sue implicazioni sulla sicurezza e sulla salute pubblica.

Sulla lotta al cambiamento climatico, che vede una accresciuta sensibilità sociale (come rilevato anche nel 53° Rapporto del CENSIS sulla situazione sociale del Paese), il cambio di paradigma che si richiede al sistema economico è complesso e ambizioso, ma può rappresentare un volano per le imprese che riescono a coglierne le opportunità, investendo in sistemi più moderni, efficienti e a minor impatto ambientale.

Con riferimento a tutti gli aspetti precedenti, è importante favorire un sempre maggiore coinvolgimento sociale. Obiettivo specifico sarà quello di migliorare la comunicazione e percezione dei rischi da parte degli individui e della collettività. In una logica di stimolo della ricerca *bottom-up*, la società civile dovrà essere coinvolta con criteri innovativi di tipo tecnologico, non-tecnologico e sociale, nello sviluppo e implementazione di piani di gestione del rischio (ad es. sismico, idrogeologico, ...) e di evacuazione della popolazione più vulnerabile. Particolare attenzione andrà rivolta alla promozione di iniziative di 'citizen science', 'çitizen ethics for resilience' e di sensibilizzazione dei cittadini, a partire dalla scuola primaria e secondaria, per rafforzare la capacità di risposta sociale a situazioni critiche per la sicurezza delle strutture e infrastrutture. Indubbiamente, un aspetto importante per il coinvolgimento delle comunità potenzialmente esposte alle conseguenze di un incidente o di un disastro, riguarda le tecnologie di comunicazione e informazione (es. i social media, e le diverse iniziative di 'citizen science' sopra menzionate). Creare e condividere informazione è un processo molto complesso, fortemente dipendente dal contesto e influenzato da fattori sociali, culturali, economici, tecnici. La ricerca in questo settore deve valorizzare le competenze delle scienze sociali e umane per costruire una maggiore consapevolezza sociale rispetto ai rischi naturali e antropici, e consentire di valutarne l'impatto sul processo di costruzione della resilienza in una comunità di persone colpite dall'emergenza, in particolare da un disastro.

Infine, l'attenzione sociale rispetto alla ricchezza del patrimonio culturale, paesaggistico e ambientale, peculiarità del nostro Paese, dovrà stimolare filoni di ricerca multidisciplinare su tecnologie, materiali, criteri di riqualificazione dell'ambiente costruito (edifici ed infrastrutture) che:

- garantiscano il pieno rispetto dei valori estetici propri delle opere, nonché dell'ambiente e del paesaggio nei quali esse sono inserite, in particolare nel caso di beni culturali, sia antichi che più recenti (es. il Ponte Musmeci in Figura 3)
- oppure siano relative ad opere che abbiano ormai esaurito il loro ciclo di vita e/o non garantiscano più standard di sicurezza accettabili.

Figura 3 Un rilevante esempio di bene culturale "moderno": il ponte Musmeci sul fiume Basento

Criteri di progettazione che coniughino sicurezza ed estetica vanno sviluppati ed applicati, naturalmente, anche alle nuove realizzazioni (es. Ponte San Giorgio a Genova, recentemente realizzato).

In conclusione, la maggiore consapevolezza sui rischi e la preparazione dei cittadini alla resilienza dovrebbe ridurre l'impatto iniziale di eventi calamitosi sulla prestazione dei sistemi grazie ad una maggiore capacità di auto-tutela delle persone e alla riduzione della vulnerabilità delle componenti strutturali esposte, aumentandone la robustezza (v. Figura 2 della Articolazione 3). La rapidità e il grado di recupero della funzionalità dei sistemi dovrebbero crescere con il grado di preparazione della società agli eventi perturbativi.

Impatti

Per le attività di ricerca da sviluppare nel campo della Sicurezza e Resilienza per la Società e lo Sviluppo Sostenibile si prevedono i seguenti impatti principali:

- Crescita della consapevolezza dei rischi, del grado di preparazione e dei comportamenti attivi dei cittadini rispetto alla gestione dei rischi e alla resilienza.
- Miglioramento della capacità di recupero a seguito di catastrofi di origine naturale (terremoti, frane, alluvioni, etc.) e antropica.
- Definizione condivisa di priorità di intervento per il miglioramento della sicurezza e resilienza in funzione delle risorse disponibili e supporto alle decisioni.
- Efficienza nell'uso delle risorse naturali in un contesto di cambiamenti climatici e sociali.
- Trasformazione di strutture e infrastrutture in chiave sostenibile garantendo la sicurezza.
- Miglioramento dell'efficienza delle reti di distribuzione dell'acqua potabile, pari al 58,6% nel 2015 (ISTAT, 2020).
- Aumento della quota di energia da fonti rinnovabili (attualmente al 17,8% per i consumi finali lordi dai dati del GSE del 2018 e 34,3% per l'energia elettrica dai dati di Terna aggiornati al 2018) fino al raggiungimento degli obiettivi fissati dal PNIEC (Piano Nazionale Integrato Energia e Clima) che prevede come obiettivo al 2030 una quota di fonti rinnovabili del 30% sui consumi finali lordi ed un contributo pari al 55% nella produzione di energia elettrica.
- Riqualificazione dell'ambiente costruito, coniugando sicurezza ed estetica.
- Diffusione della consapevolezza e dei comportamenti attivi dei cittadini per la sicurezza delle proprie abitazioni, anche utilizzando in modo più ampio e responsabile incentivi pubblici.
- Miglioramento della sicurezza della rete ferroviaria.
- Riduzione delle emissioni di gas serra.
- Generale incremento degli investimenti in prodotti di proprietà intellettuale e in ricerca e sviluppo.
- Generale incremento dell'intensità di ricerca nella società italiana.

Interconnessioni

Le interconnessioni con altri Ambiti Tematici, maggiormente riconducibili a questa Articolazione di ricerca, sono più evidenti con gli AT:

- PATRIMONIO CULTURALE: il valore inestimabile dei beni culturali, architettonici e ambientali del nostro Paese, riconosciuto dall'UNESCO, impone una sensibilità particolare negli interventi di messa in sicurezza di strutture e infrastrutture spesso sedimentate su stratificazioni storiche millenarie. Basti pensare al paesaggio antropico che ancora oggi ricalca in buona parte lo sviluppo della rete viaria romana e medioevale. Ne consegue che la riqualificazione strutturale e la rigenerazione necessaria per migliorare la sicurezza, e le prestazioni in generale, richiedono un approccio multidisciplinare che coinvolge esperti di scienze umane, architettura, arte, paesaggio. È anche un'opportunità unica per sviluppare e affermare una specificità della ricerca italiana nella conservazione e restauro dell'ambiente costruito che sia in grado di coniugare sicurezza e valore estetico.
- SICUREZZA SISTEMI NATURALI: in questo ambito tematico l'attenzione si focalizza sulla sicurezza delle strutture, infrastrutture e reti sollecitate da forzanti naturali (terremoti, frane, alluvioni) e sul miglioramento della capacità di recupero (resilienza) a seguito del loro impatto. Centrale è sviluppare una riflessione condivisa ("interconnessa") sul rischio accettabile dalla società e sugli investimenti necessari per raggiungere il grado di sicurezza 'contrattato' con i cittadini e stabilito dalle normative sulla sicurezza delle strutture e infrastrutture, sul rischio sismico, alluvionale, etc.
- CAMBIAMENTI CLIMATICI E ADATTAMENTO: nell'ambito tematico 3.1 si pone l'accento sulla sicurezza delle infrastrutture per la mitigazione del cambiamento climatico come i sistemi di generazione, trasporto, utilizzo, stoccaggio dell'energia. Attenzione è riferita anche a misure di adattamento come l'uso più efficiente delle risorse idriche e naturali per migliorare la sicurezza della catena agroalimentare.

Key Performance Indicators

La qualità dei risultati della ricerca e degli impatti raggiunti potrà essere valutata mediante specifici indicatori, tra i quali:

- Grado di conoscenza dei cittadini della normativa vigente in termini di sicurezza di strutture, infrastrutture e reti.
- Iniziative di "citizen science" organizzate sul territorio nazionale, come sportelli della scienza, caffè-scienza, osservatori dei cittadini, contratti di fiume, etc.
- Indicatori della Strategia Nazionale per lo Sviluppo Sostenibile del MATTM (2017) e definiti dall'ISTAT (2020) in relazione al raggiungimento dei 17 SDGs dell'Agenda 2030.
- Investimenti in prodotti di proprietà intellettuale sugli investimenti totali (17.3% nel 2019, secondo ISTAT, 2020).
- Numero di ricercatori per abitante (2.32 ogni 1000 abitanti nel 2017).
- Percentuale di persone in abitazioni con problemi strutturali o di umidità (13.2%, nel 2018).
- Percentuale di persone esposte al rischio di alluvioni o frane (10.4% e 2.2% rispettivamente, nel 2018).
- Emissioni di CO2 e altri gas climalteranti per abitante (7.3 ton CO_2 equivalente nel 2018).

Alcuni documenti di riferimento

Camera dei Deputati, Servizio Studi, 2020. La Comunità internazionale e l'attuazione dell'Agenda globale per lo sviluppo sostenibile, https://www.camera.it/temiap/documentazione/temi/pdf/1105015.pdf

CENSIS Centro Studi Investimenti Sociali, 2019. 53° Rapporto sulla situazione sociale del Paese, Roma.

European Commission, Orientations towards the first Strategic Plan for Horizon Europe, Dicembre 2019, 2019-Dec_EC-RTD_Orientations_H-EU_strategic-plan.pdf.

ISTAT, Rapporto SDG2, 2020. Informazioni statistiche per l'Agenda 2030 in Italia, 2020. https://www.istat.it/it/files//2020/05/SDGs_2020.pdf

Ministero dell'Ambiente e della Tutela del Territorio e del Mare, 2017. Strategia Nazionale per lo Sviluppo Sostenibile.

UNDRR, United Nations Office for Disaster Risk Reduction, 2015. Sendai Framework for Disaster Risk Reduction 2015-2030, https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030

Strategia Energetica Nazionale SEN 2017 del MiSE e MATTM, 2017.

Piano nazionale energia e clima 2030 (PNIEC 2030) del MiSE, 2020.

Appendice 1

All'interno delle quattro Articolazioni strategiche, vanno considerate specifiche linee di ricerca, un elenco (non esaustivo) delle quali è riportato in Tabella A.1.

1.	**Analisi e Valutazione dei Rischi e della Resilienza**
1.1.	Pericoli attuali, emergenti e multipli (naturali e antropici)
1.2.	Pericoli transnazionali
1.3.	Effetti a cascata ed effetti domino
1.4.	Eventi naturali estremi
1.5.	Accumulo del danno, degrado e invecchiamento
1.6.	Analisi del ciclo di vita per la progettazione di sistemi resilienti e sostenibili
1.7.	Patrimonio edilizio diffuso
1.8.	Infrastrutture fisiche per la distribuzione di persone, materie e servizi
1.9.	Reti di approvvigionamento e logistiche
1.10.	Reti complesse
1.11.	Sistemi di sistemi
1.12.	Sistemi cyber-fisici
1.13.	Security fisica delle infrastrutture per la distribuzione di persone, materie e servizi
1.14.	Modelli logici, stocastici e di simulazione per la sicurezza e la resilienza
1.15.	Modelli di rischio per la sicurezza e la resilienza
1.16.	Modelli di crisi per la sicurezza e la resilienza
1.17.	Modelli economici per la sicurezza e la resilienza
1.18.	Metriche per la sicurezza e la resilienza di ausilio alla pianificazione di infrastrutture critiche
2.	**Metodi, Tecniche e Tecnologie per il Monitoraggio e la Prevenzione dei Rischi**
2.1.	Progettazione integrata di sistemi complessi
2.2.	Instrument Fault Detection, Isolation and Accommodation (IFDIA schemes)
2.3.	Strumenti autonomi, rover, droni e robot per la gestione della sicurezza di strutture e infrastrutture
2.4.	Sistemi di monitoraggio e controllo di infrastrutture critiche
2.5.	*Wide Area Measurement Systems and Wide Area Control systems*
2.6.	*Resiliency control e* Sistemi *Self-healing*
2.7.	Sistemi di monitoraggio per la misura del degrado ed invecchiamento di infrastrutture
2.8.	Big data e data science per la sicurezza e la resilienza di infrastrutture interdipendenti e sistemi complessi
2.9.	Intelligenza distribuita per la sicurezza e la resilienza di infrastrutture interdipendenti e sistemi complessi
2.10.	Intelligenza artificiale e machine learning per la sicurezza di infrastrutture interdipendenti e sistemi complessi
2.11.	Sistemi e tecnologie early warning per la gestione dei rischi naturali ed antropici
2.12.	Remote sensing e satellite radar interferometry learning per la sicurezza di infrastrutture interdipendenti e sistemi complessi
2.13.	Sistemi satellitari a basso costo per le infrastrutture critiche
2.14.	Nuove architetture di rete e nuovi servizi per la sicurezza e la resilienza delle infrastrutture critiche
3.	**Gestione dei Rischi e della Resilienza**
3.1.	Modelli, metodi e tecniche di preparazione all'emergenza (preparedness)
3.2.	Modelli, metodi e tecniche di risposta alla crisi nel breve e medio termine
3.3.	Algoritmi di ottimizzazione delle barriere preventive, mitigative, emergenziali e reattive
3.4.	Barriere preventive, mitigative, emergenziali, reattive
3.5.	Progettazione integrata di sistemi complessi
3.6.	Progettazione di reti interconnesse
3.7.	Progettazione di strutture e infrastrutture ed economia circolare
3.8.	Governance della resilienza
3.9.	Gestione delle risorse per la resilienza a breve termine
3.10.	Metodi e tecnologie per la valutazione del rischio residuo e rischio accettabile di infrastrutture e sistemi complessi

3.11.	Pianificazione delle linee di difesa in emergenza, preparedness, readiness
4.	**Sicurezza e Resilienza per la Società e lo Sviluppo Sostenibile**
4.1.	Modellazione dei comportamenti sociali per la resilienza
4.2.	Etica, equità, e sostenibilità della resilienza
4.3.	Azioni preventive per territori poco sviluppati
4.4.	Azioni preventive per categorie fragili
4.5.	Informazione e comunicazione del rischio
4.6.	Ruolo ed Azione dei Cittadini nella sicurezza e resilienza
4.7.	Responsabilità sociale e uso razionale delle risorse (es. idriche, energetiche)

Tabella A.1. Elenco (non esaustivo) di linee di ricerca specifiche all'interno delle quattro Articolazioni strategiche di ricerca.

3.2 Sicurezza sistemi naturali

Analisi critica del contesto di riferimento, dalla ricerca fondamentale all'applicazione

L'analisi del gruppo di lavoro sul tema Sicurezza per i Sistemi Sociali - Sicurezza Sistemi Naturali ha sviluppato l'analisi critica del contesto (interno ed esterno) nonché la definizione delle articolazioni seguendo un approccio analitico organizzato su varie fasi:

- raccolta di documentazione scientifica focalizzata sulle dinamiche evolutive del settore;
- definizione delle necessità prioritarie della ricerca e innovazione del sistema nazionale, anche alla luce degli impatti attesi elencati nel work program di Horizon Europe;
- condivisione di un set di articolazioni che il gruppo di lavoro ha valutato come strategiche per un avanzamento significativo della ricerca nel nostro Paese;
- compilazione delle schede sintetiche ed estese per ciascuna delle articolazioni individuate.

Principali scenari evolutivi nel campo della sicurezza dei sistemi naturali, ruolo atteso per nuove tecnologie e rilevanza rispetto alle transizioni ambientale, digitale, economica, energetica e sociale

La prevenzione e la mitigazione dell'impatto dei rischi naturali ha una rilevanza sociale ed economica immediata per il nostro Paese, essendo l'Italia uno dei paesi europei più esposti ai rischi naturali: geologico, sismico, vulcanico, geochimico, mineralogico, geomorfologico, idrologico, idraulico, meteorologico. In media, vi sono una ventina di terremoti distruttivi al secolo; le eruzioni sono poco frequenti ma potenzialmente devastanti, anche nel breve termine; le frane note sono oltre 600.000 (mediamente due ogni km^2); le inondazioni sono comuni sia in ambiente di pianura che montano; 1/3 delle coste ha problemi di erosione e le restanti in larga parte si trovano in condizioni di stabilità dovuta a interventi di protezione talvolta conflittuali con le dinamiche naturali; la posizione al centro del Mediterraneo rende l'Italia particolarmente sensibile ai cambiamenti climatici che inducono desertificazione, perdita di territorio e aumento della concentrazione salina nelle acque superficiali e sotterranee dovuto a estrazioni idriche non più compensate dalle precipitazioni. Negli ultimi cinquanta anni (1967-2016), i terremoti, le frane e le inondazioni hanno causato oltre 6.700 vittime e centinaia di migliaia di sfollati e senza tetto. I terremoti verificatisi dal 1968 (Belice) al 2017 (Centro Italia) hanno causato 4.948 morti (di cui 2.914 in Irpinia) e 515.200 senza tetto. Dal 1970 al 2019, frane e inondazioni hanno causato 1.733 morti e dispersi, 1.923 feriti, 320.028 evacuati e senza tetto in 3.786 località colpite. Le sole spese pubbliche per i disastri naturali in Italia sono stimate in circa 240 miliardi di Euro tra il 1944 e il 2012 (circa 3,5 miliardi di Euro all'anno a prezzi del 2011), di cui circa 20 miliardi di Euro nel periodo 2010-2012. La spesa dello Stato per gli otto principali terremoti che hanno colpito l'Italia tra il 1968 ed il 2017 è pari a 129 miliardi di Euro (prezzi 2014). Le risorse complessivamente stanziate per i sismi più recenti di Abruzzo 2009, Emilia-Romagna 2012 e Centro Italia 2016-2017, sono state 38,8 miliardi di Euro (per il 2009-2047). Nel periodo 2002-2017, il FSUE (Fondo di Solidarietà della UE) ha erogato a favore del nostro Paese 2,5 miliardi di Euro, corrispondente a oltre il 40% di tutte le erogazioni del fondo. A questi dati vanno aggiunti circa 14 miliardi di euro di danni da calamità naturali riconosciuti al settore agricolo nel 2003-2012. Agli stanziamenti di bilancio pubblico vanno sommati inoltre significativi costi indiretti e non riconosciuti, anche perché poco documentati, come l'interruzione di attività produttiva, i costi personali non risarciti, la perdita di beni culturali e di luoghi identitari, e le perdite per il turismo.

In questo contesto, la ricerca sui rischi naturali deve avere un ruolo di primo piano e contribuire significativamente al benessere sociale ed economico del Paese partecipando attivamente al complesso sistema di contrasto e governance dei rischi naturali e delle loro conseguenze. Essa può svolgere compiti di supporto tecnico-scientifico in parte normati dalla legislazione, e mettere a disposizione capacità scientifico-tecnologiche e umane che potranno fornire nuovi ed importanti strumenti per la riduzione dei costi umani e materiali. In particolare, la ricerca italiana potrà

produrre in futuro importanti avanzamenti nell'ambito della prevenzione e aumento della resilienza ai rischi naturali, che rappresentano le aree di investimento con maggiore ritorno in termini di costi evitati umani, sociali ed economici. A tal fine, gli orientamenti di ricerca proposti per il PNR 2021-2027 comprendono, oltre all'avanzamento della ricerca fondamentale, dei sistemi di monitoraggio e delle strategie multi-rischio, anche la ricerca a supporto della governance dei rischi e il coinvolgimento dei cittadini attraverso lo sviluppo di approcci di 'citizen science', in linea con gli orientamenti della ricerca europea.

Nella declinazione degli indirizzi proposti nelle articolazioni seguenti, il Gruppo di Lavoro Sicurezza Sistemi Naturali ha seguito gli orientamenti della ricerca europea ed italiana sottolineando l'importanza della ricerca di base nello sviluppo di tutte le discipline coinvolte e la necessità di una forte sinergia ed una maggiore integrazione fra ricerca fondamentale e applicata.

Rilevanza nel contesto associato alle politiche europee, generali e di ricerca

La ricerca sui rischi naturali contribuisce alla realizzazione in Italia delle strategie di alto livello dell'Unione Europea e degli orientamenti della ricerca europea di Horizon Europe.

La 'transizione di sostenibilità' (Sustainability Transition) è al centro del programma della nuova Commissione Europea. Lo European Green Deal (EGD), nel perseguire l'obiettivo di fare dell'Unione la prima regione 'carbon neutral' al mondo, copre un'ampia gamma di interventi per la conservazione delle risorse naturali e ambientali dell'Unione. Nello EGD (EC 2019)[3] si afferma l'obiettivo di "proteggere, conservare e migliorare il capitale naturale dell'Unione, e proteggere il benessere e la salute dei cittadini dai rischi e dagli impatti legati all'ambiente". Nell'ambito dello EGD, la Commissione adotterà una nuova e più ambiziosa strategia di adattamento al cambiamento climatico rivolta all'aumento di resilienza e prevenzione, all'inclusione del rischio climatico nelle decisioni pubbliche e private, all'adozione di 'nature-based solutions'. Investitori e sistema finanziario, imprese, cittadini, città dovranno essere supportati per sviluppare le loro strategie attraverso l'accesso ai dati e alla conoscenza necessaria. Nell'ambito del 'Sustainable Europe Investment Plan' (EC 2020)[4], che dovrà fornire risorse specifiche per la transizione, la Commissione proporrà forme di 'condizionalità ambientale' per i programmi e i progetti. Le conclusioni del Consiglio Europe del 21 luglio 2020, che ha raggiunto l'accordo sul finanziamento della strategia di ripresa post-COVID-19 (Next Generation EU e Bilancio dell'Unione 2021-2027), hanno confermato sia gli orientamenti dello EDG sia l'indirizzo di dedicare il 30% del Bilancio dell'Unione a spese e investimenti connesse al cambiamento climatico, anche nell'ambito dello sviluppo regionale dove hanno grande peso gli investimenti per l'assetto territoriale.

Nell'ambito delle politiche europee di ricerca, gli orientamenti di Horizon Europe, presentati nello Strategic Plan del dicembre 2019 e nel suo sviluppo in corso, si collegano con enfasi alla 'sustainability transition', inclusa la gestione dei rischi naturali, nei seguenti termini: "[...] azioni per affrontare queste sfide saranno sostenute da un'ampia gamma di attività nel Pilastro II, come lo sviluppo di nuovi indicatori di sviluppo sostenibile (Cluster 2); una miglioramento della gestione dei rischi naturali, come i rischi climatici e gli eventi estremi (Cluster 3); la combinazione dell'osservazione del sistema terra dallo spazio con gli avanzamenti del digitale per fornire dati utili alla mitigazione (Cluster 4); la protezione dei cittadini dall'inquinamento (Cluster 1); attività di ricerca e innovazione rivolte a fornire soluzioni per una società clima-neutrale e resiliente [...] (Clusters 4, 5 and 6)."[5]

---

[3] European Commission (2019a). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions 'The European Green Deal', COM (2019)640 final

[4] European Commission (2020a). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions 'Sustainable Europe Investment Plan - European Green Deal Investment Plan', COM(2020)21final.

[5] Orientations towards the first Strategic Plan for Horizon Europe, December 2019, https://ec.europa.eu/info/sites/info/files/research_and_innovation/strategy_on_research_and_innovation/documents/ec_rtd_orientations-he-strategic-plan_122019.pdf

In particolare, il Cluster 3 'Civil security for society' prevede lo sviluppo di ricerca per una "migliore gestione dei rischi naturali e un aumento della resilienza sociale" attraverso una "migliore comprensione dei disastri naturali ed antropici e lo sviluppo di nuovi concetti e tecnologie per contrastare tali rischi". Si afferma inoltre che "I cittadini e le comunità devono essere coinvolti nel rendere le società più resilienti attraverso la ricerca e l'innovazione tecnologica, non tecnologica e sociale. Le scienze sociali (SSH - Social Sciences and Humanities) devono essere integrate nella ricerca sulla sicurezza, anche, quando necessario, nella ricerca sulle tecnologie. Inoltre, una migliore conoscenza dei fattori umani e sociali può aiutare a raggiungere gli impatti desiderati. A tal fine, la Commissione continuerà a chiedere una 'Societal Impact Table' come parte del processo di presentazione e valutazione dei progetti."

Tra gli orientamenti desiderabili di ricerca e innovazione vi è quello della trasversalità: "La ricerca e innovazione orientata fronteggia questioni trans-settoriali e di governance dei rischi naturali che presentano dei trade-off nella definizione delle politiche. Ciò comprende non solo la protezione civile come tale, ma anche le aree collegate della gestione del territorio, dello sviluppo agricolo e rurale, dell'ambiente, del clima e dell'energia. La ricerca deve contribuire alla creazione di metodologie per infrastrutture 'resilient by design'. Come risultato di una migliore conoscenza dei fattori umani e sociali, la ricostruzione post-disastro può rispettare i valori tradizionali e i criteri di qualità di intervento richiesti dai siti culturali". Per quanto riguarda in particolare i rischi naturali "Dato il devastante potenziale di tali disastri, la ricerca e innovazione deve sostenere una migliore preparazione ex ante e una migliore risposta agli eventi. Ciò include migliori e più tecnologicamente avanzate capacità di protezione civile."

Nell'ambito delle Mission di Horizon Europe, secondo i primi risultati disponibili (luglio 2020), emergono forti orientamenti di multidisciplinarità e coinvolgimento dei cittadini, con particolare riferimento al Mission Board 'Adaptation to climate change including societal transformation', indica il seguente target "Entro il 2030, tutte le amministrazioni locali e le regioni avranno accesso alla conoscenza dei propri profili di rischio climatico e a migliori sistemi di 'early warning' per tutti i rischi rilevanti, avranno adottato piani integrati di gestione del rischio climatico, e avranno infrastrutture e servizi che sono sicuri, operabili, e accessibili anche in condizioni critiche ". [6] A tal fine, si indica la necessità di: "[...] mobilitare la ricerca e l'innovazione verso i bisogni di conoscenza, tra cui: i modelli del Sistema Terra di nuova generazione con risoluzioni migliori e più granulari e una migliore capacità di proiezione climatica; la valutazione di rischi cumulativi e a cascata; le perdite indirette e intangibili; gli effetti di propagazione e diffusione attraverso le catene di valore e le reti sociali ed ecologiche; i processi sociali e culturali che plasmano il modo in cui i rischi e le incertezze sono percepiti ed affrontati; il legame tra salute, ambiente e cambiamento climatico". Inoltre, è necessario: "facilitare il co-design delle soluzioni. Per migliorare la rilevanza dei dati e della conoscenza, l'usabilità dei servizi digitali e la praticabilità delle soluzioni, la Mission richiederà ai cittadini e agli stakeholder di essere coinvolti nella co-produzione di dati e conoscenza, nel co-design dei servizi climatici e delle soluzioni attuabili, anche attraverso lo sviluppo di 'citizen science'."

Rilevanza rispetto al contesto nazionale

L'analisi del contesto nazionale rivela come la ricerca sulla Sicurezza dei Sistemi Naturali condivida l'opportunità di combinare in modo interdisciplinare una molteplicità di settori per un utilizzo integrato ed efficace delle risorse, per lo sviluppo sostenibile, per una migliore capacità di adattamento ai cambiamenti globali, e per ridurre i rischi per l'ambiente, la società e l'economia. In tale contesto, l'acquisizione di nuove conoscenze, modelli, e strumenti operativi rappresenta anche un importante volano industriale.

Per la **riduzione dei rischi (*Disaster Risk Reduction*, DRR)** è opportuno sviluppare metodologie e sistemi finalizzati alla previsione, valutazione e mitigazione dell'impatto di eventi potenzialmente dannosi, che devono essere affiancati da ricerche (a) per migliorare le capacità previsionali dei fenomeni, inclusi studi sui precursori (sismici, vulcanici, geomorfologici, di frana, meteorologici, ecc.); (b) per una corretta valutazione, gestione e comunicazione delle incertezze; (c) per l'aggiornamento/completamento di sistemi informativi territoriali (cartografia geologica, delle faglie capaci, delle frane, del rischio alluvioni, inventario del patrimonio edilizio ed infrastrutturale, inventario

[6] https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=40023&no=1

dei beni naturalistici e culturali sottoposti a tutela), anche utilizzando sistemi di osservazione integrati (satelliti, droni, misure a terra); (d) per la valutazione quantitativa della pericolosità e del rischio posto dai diversi fenomeni naturali, anche in un contesto *multi-hazard/risk*; (e) per la stima dell'impatto che i cambiamenti climatici, ambientali, economici e sociali hanno e potranno avere su diverse tipologie di pericolosità, a differenti scale spaziali e temporali; e (f) per l'uso ottimale delle nuove conoscenze per la riduzione del rischio e l'incremento della resilienza, anche in relazione alla progettazione di piani emergenziali e servizi di soccorso, di protezione e difesa civile.

È indispensabile conoscere meglio come funziona l'intero **sistema Terra**, adottando una visione olistica e interdisciplinare per la comprensione dei meccanismi che regolano i fenomeni complessi che ne caratterizzano la dinamica, controllando le interazioni tra litosfera, idrosfera, criosfera, biosfera, atmosfera, ionosfera e magnetosfera. Una approfondita e puntuale conoscenza del territorio e dei processi evolutivi a questo associati, si pone come elemento chiave per lo sviluppo e l'evoluzione di modelli per la valutazione della pericolosità, che a loro volta contribuiranno a stime più affidabili delle conseguenze degli eventi: in tempo reale (*early warning*), nel breve termine (per la gestione delle emergenze) e nel lungo termine (per la pianificazione territoriale). La diversità e ricchezza del patrimonio geologico (*geoheritage*) italiano richiedono ricerche per una migliore gestione del territorio. Nuove conoscenze permetteranno di incidere sui sistemi socio-economici, realizzando una società più reattiva e resiliente ad affrontare le future calamità naturali. Per raggiungere tali obiettivi, è essenziale la collaborazione tra Enti di ricerca, Università, industria, istituzioni e cittadini. I ricercatori italiani hanno le competenze per far fronte alle sfide delle geoscienze e dell'ingegneria civile, ambientale e del territorio, ricostruendo l'interno del pianeta, i meccanismi che ne controllano l'evoluzione dinamica, le interazioni tra i vari comparti del sistema Terra (solida e fluida), le trasformazioni della superficie, le conseguenze dei cambiamenti climatici e ambientali, gli effetti dell'industrializzazione sul sottosuolo, il mare, l'atmosfera e la biodiversità, nonché gli effetti indotti sull'ambiente costruito e più in generale antropizzato, a partire dallo studio della sua esposizione e vulnerabilità. È necessario realizzare un'infrastruttura integrata capace di mappare in 3D il sottosuolo del territorio nazionale, di modellare e monitorare i processi endogeni ed esogeni che ne regolano la dinamica, e di verificare e prevedere gli impatti dei cambiamenti, nel breve e lungo periodo. È imprescindibile lo sviluppo e la manutenzione di reti osservative, multi-parametriche e integrate (meteo-idro-geologiche, geofisiche, geodetiche, satellitari, gravimetriche, magnetiche, ionosferiche, idro-geochimiche, abiotiche-biotiche, della biodiversità) e che siano integrate ai più recenti prodotti satellitari delle missioni Copernicus Sentinel, SMAP, SMOS e SWOT. È altrettanto necessario che i dati raccolti dalle reti siano organizzati e gestiti secondo i principi dell'open science.

Obiettivi 2021-2027: le grandi sfide per la ricerca e l'innovazione nell'ambito della sicurezza dei sistemi naturali

L'obiettivo prioritario del PNR in ambito Sicurezza sistemi naturali è quello di promuovere sia la **ricerca di base** che quella **applicata**. Per la **ricerca di base**, l'innovazione dovrà prevedere un ***framework* comune** per l'avanzamento e l'uso delle conoscenze sui processi che governano le dinamiche evolutive dei rischi naturali e per la loro previsione e prevenzione, nel contesto dei cambiamenti (climatici, ambientali, sociali, economici) in corso e attesi. L'area mediterranea offre l'opportunità di quantificare le variazioni in atto negli ecosistemi terrestri e marini. Si ritiene strategico un rafforzamento degli studi in aree polari, considerato il loro ruolo nel bilancio globale dei fenomeni climatici e per le dinamiche degli oceani, dell'atmosfera e della magnetosfera. Un *framework* comune potrà agevolare la condivisione delle conoscenze. È di importanza critica programmare investimenti per il miglioramento delle reti di monitoraggio e osservative, multi-parametriche e integrate, anche tramite le più avanzate tecnologie ICT. La **ricerca applicata** dovrà produrre conoscenze e innovazioni utili ad attori **istituzionali** e **industriali**. In questo risulta prioritario:

a) **Conoscenza di Base, Processi e Modelli**. Favorire sviluppi significativi della ricerca di base sui processi coinvolti nell'evoluzione dei fenomeni naturali associati al sistema terra e del loro feedback con azioni antropogeniche, sulla identificazione e rappresentazione di eventuali fattori ed eventi preparatori e precursori e sulla loro modellazione, per una più avanzata definizione di scenari di pericolosità e di rischio;

b) **Monitoraggio dei sistemi naturali**. Innovare le basi dati, rendendole fruibili ed integrabili con moderni strumenti modellistici, anche includendo tecniche strumentate da intelligenza artificiale;
c) **Strategie Multi-Rischio per la difesa da eventi naturali**. Sviluppare il monitoraggio multiparametrico proponendo strumenti e tecnologie di acquisizione dati innovativi al suolo e da satellite, includendo lo sviluppo e la sperimentazione di tecnologia avanzata per sistemi di early warning multirischio dei fenomeni naturali;
d) **Governance e Gestione dei Rischi Naturali e degli Impatti Antropici**. Migliorare la quantificazione e la comunicazione dei risultati ottenuti nella stima della pericolosità e del rischio e della relativa incertezza. Migliorare le basi scientifiche per le decisioni e gli investimenti, pubblici e privati, in mitigazione e prevenzione

Il conseguimento di tali obiettivi è strategico nel contesto nazionale ed internazionale, e potrà avvenire a seguito di significativi investimenti per lo sviluppo dell'integrazione di strumenti di varia natura che includono, ad esempio, (*a*) tecnologie e sistemi di monitoraggio, *in-situ* e da remoto; (*b*) sistemi e strumenti per l'elaborazione e la modellazione (concettuale, analitica e numerica) fisicamente basata di fenomemi naturali, dati e informazioni multiparametriche; (*c*) tecniche di *data analysis* applicate a *big data*; (*d*) sistemi e strumenti per l'individuazione di possibili condizioni di criticità locali e a scala nazionale; e (*e*) modellistica multidisciplinare integrata con le dimensioni sociali ed economiche del rischio

I KPI per la quantificazione del raggiungimento degli obiettivi 2021-2027

Il raggiungimento degli obiettivi di ricerca descritti nelle 4 articolazioni possono essere misurati attraverso indicatori di risultato e di esito. Si è ritenuto opportuno identificare insiemi di indicatori differenti in funzione del grado di TRL associato alle 4 articolazioni individuate. A titolo di esempio, si riportano alcune proposte di indicatori nella tabella seguente.

TRL atteso / Articolazione	Indicatori di risultato	Indicatori di esiti
Grado elevato di TRL	Indicatori bibliometrici (pubblicazioni scientifiche di qualità secondo criteri comunemente riconosciuti). Indicatori di trasferimento tecnologico (brevetti italiani/internazionali; spin off e start up) Indicatori di progetto (e.g., piattaforme per basi dati implementate e fruibili; strumenti computazionali approntati; raggiungimento livello operativo rete di monitoraggio; % obiettivi tecnologici conclusi nei tempi stabiliti)	Indicatori di trasferimento tecnologico (brevetti italiani/internazionali; spin off e start up). Sul versante sociale/community: misure di social acceptance e citizen-reported experience raccolti su casi studio In ambito ricerca (come leadership internazionale): numero di progetti EU nell'ambito dei quali la tecnologia sviluppata da UO italiane è utilizzata; In ambito industriale: coinvolgimento/interesse/dimensione del settore industriale (e.g., enti/società gestione territorio/ambiente/acqua) e della gestione pubblica (e.g., ARPA ...) in Italia nella implementazione/fruizione delle tecnologie sviluppate.
Grado modesto/basso di TRL	Indicatori bibliometrici (pubblicazioni scientifiche di qualità secondo criteri comunemente riconosciuti).	Indicatori di trasferimento tecnologico (brevetti italiani/internazionali; spin off e start up) Sul versante ricerca (leadership internazionale): numero di progetti EU o di respiro internazionale guidati da (o a cui partecipano) UO italiane

Articolazione 4	Indicatori bibliometrici (pubblicazioni scientifiche di qualità secondo criteri comunemente riconosciuti). Numero di report di valutazione di tecnologie, procedure e servizi a queste associate Indicatori di public engagement (disseminazione scientifica, informazione/formazione, tavoli di confronto con stakeholders del settore ambientale e altri settori, con la sfera dei decisori pubblici e delle associazioni di cittadini).	Sul versante public engagement: diffusione di misure di sicurezza e gestione rischi naturali, di misure di gestione degli impatti antropici; inserimento e condivisione di nuove tecnologie e conoscenze in livelli decisionali e adozione di risultati di ricerca all'interno di linee guida/protocolli/piani emergenziali, anche con riferimento alla sostenibilità delle infrastrutture.

Dal punto di vista generale, si osserva come la ricerca sul monitoraggio dei sistemi naturali ha effetti immediati e diretti sulla società. Conseguentemente i risultati della ricerca devono essere diffusi alla popolazione mediante un'educazione il più possibile scientificamente basata e rigorosa per garantire la condivisione della consapevolezza e sicurezza di vivere in un ambiente naturale o antropico in sicurezza.

In questo contesto, una delle *KPI* in comune a tutte le Articolazioni incluse nel Gruppo di lavoro risulta:

- Trasferimento delle conoscenze verso la cittadinanza e controllo della ricezione da parte di questa;

Altri *KPI* che in generale sono collegabili agli aspetti scientifici delle articolazioni includono:

- Rispondenza alla tempistica di realizzazione dei progetti: rispetto delle scadenze nel completamento dei pacchetti di lavoro e/o dei tasks, utilizzazione delle risorse per ogni step di lavoro, giustificativi per i cambiamenti richiesti nel budget o nei tempi di realizzazione;
- Rispondenza ai formati richiesti: standard informatici, format per report intermedi e finali, determinazione delle milestone e dei prodotti del progetto;
- Percentuale di rispondenza dei risultati raggiunti rispetto a quelli attesi/previsti dalle attività di ricerca;
- Percentuale di rispondenza al budget programmato in relazione ai risultati attesi.

Articolazione 1. Conoscenza di base, processi e modelli

La prima articolazione include, come elemento prioritario di attenzione dell'ambito tematico, attività di ricerca, coadiuvata da innovazione tecnologica, finalizzata all'avanzamento della conoscenza dei processi chimico-fisici caratterizzanti i sistemi naturali e connessi ai fenomeni determinanti le condizioni di pericolosità e rischio.

Un'approfondita conoscenza della dinamica evolutiva dei sistemi naturali, unitamente all'ulteriore sviluppo delle moderne tecnologie di monitoraggio (articolazione 2) e computazionali costituiscono condizione imprescindibile per il miglioramento e lo sviluppo di modelli innovativi utilizzabili per la previsione e la gestione dei rischi naturali.

Particolare attenzione dovrebbe essere rivolta al miglioramento delle prestazioni dei modelli per quanto riguarda la quantificazione e la riduzione dell'incertezza nelle simulazioni, anche al fine di incrementarne l'affidabilità in contesti di early warning.

A tal fine è auspicabile che approcci modellistico-numerici deterministici e probabilistici, fisicamente basati e di intelligenza artificiale siano adeguatamente orchestrati per progettare modelli di simulazione versatili e adattabili, per complessità e dati richiesti, ai diversi e specifici contesti che caratterizzano gli scenari di rischio nei sistemi naturali.

Obiettivi

L'avanzamento significativo delle conoscenze dei processi che governano i diversi ambiti dell'intero sistema Terra è un elemento chiave per consentire sviluppi significativi di schemi interpretativi e di modelli, anche multidisciplinari,

per la valutazione della pericolosità degli eventi. Questo contribuirà ad accrescere ulteriormente il livello di competitività del paese, garantendo una affidabile valutazione delle possibili ricadute dei rischi naturali su diverse scale temporali rispondenti ad esigenze di early warning, gestione delle emergenze e pianificazione territoriale.

Come indicato precedentemente, diventa prioritario in tale contesto promuovere infrastrutture integrate finalizzate alla mappatura esaustiva del sottosuolo a livello nazionale, al monitoraggio dei processi che ne regolano la dinamica, anche con riferimento agli strumenti associati all'Articolazione 2.

La ricerca di base è indubbiamente il pilastro su cui approfondire studi applicati per costruire una società resiliente ai rischi naturali e in grado di utilizzare le risorse naturali in modo sostenibile.

La conoscenza dei meccanismi evolutivi del pianeta sono il prerequisito per l'innovazione che preveda l'avanzamento e l'uso delle conoscenze sulle risorse, l'ambiente, i rischi naturali e la loro previsione e prevenzione, nel contesto dei cambiamenti (climatici, ambientali, sociali, economici) in corso e attesi.

Comunità diverse tendono a trattare i problemi in modo "proprio", con linguaggi e strumenti diversi, con scarse interazioni con altre comunità scientifiche e con limitato collegamento all'industria. Un framework comune renderà più facile la condivisione delle conoscenze.

È richiesto un completamento ed aggiornamento della base di dati del territorio italiano ed è importante favorire lo sviluppo e la manutenzione di reti osservative, multi-parametriche e integrate, come previsto nell'articolazione 2 (meteo-idro-geologiche, geofisiche, geodetiche, satellitari, gravimetriche, magnetiche, ionosferiche, idro-geochimiche, abiotiche-biotiche, della biodiversità). È altrettanto necessaria la ricerca sperimentale finalizzata alla comprensione dei processi a tutte le scale spaziali e temporali.

È fondamentale che i risultati sperimentali e i dati raccolti dalle reti siano organizzati e gestiti secondo i principi dell'open science al fine di una rapida ed efficace condivisione incentivante studi multidisciplinari, necessari nell'analisi dei rischi naturali.

Per la mitigazione del rischio sismico, la ricerca è auspicabile si focalizzi sullo sviluppo di modelli che considerino adeguatamente la fisica della sorgente e la propagazione delle onde, integrando approcci statistici, geologici, fisici e ingegneristici. È necessario un miglioramento delle conoscenze sui fenomeni di nucleazione, di propagazione delle onde, e modificazione del campo d'onda dovuto a effetti di amplificazione locali. L'attuale approccio alla progettazione strutturale non garantisce uniformità del rischio tra costruzioni dello stesso tipo in siti a pericolosità diversa e tra tipologie strutturali diverse progettate nello stesso sito; vanno pertanto riviste le filosofie alla base della definizione e gestione del rischio. Per quanto riguarda il patrimonio costruito, serve perseguire una nuova ricerca su sistemi di mitigazione attraverso la riduzione dell'esposizione, a larga scala. Analoghe ricerche sono necessarie per capire l'evoluzione effusiva o esplosiva e relativi volumi dei vulcani.

Per la mitigazione dei rischi geo-idrologici e idraulici (da frana, da colata di detrito, da inondazione, ecc.), la ricerca dovrà puntare al miglioramento delle capacità previsionali, a tutte le scale spaziali e temporali, con particolare riferimento alle aree montane, sedi privilegiate di fenomeni impulsivi e alle aree urbane dove la fitta trama del "costruito" interseca e condiziona l'evoluzione dei fenomeni. Dovrà essere considerata la non stazionarietà delle forzanti, dovuta ai cambiamenti climatici e ambientali in atto e attesi. Dovranno infine essere migliorate le capacità previsionali per la stima degli impatti economici, ambientali e sulla popolazione dei rischi geo-idrologici e idraulici, e ulteriormente migliorati gli strumenti urbanistici. I cambiamenti dell'uso del suolo e l'aumento della pressione antropica sul territorio hanno determinato l'alterazione della risposta idrologica dei bacini idrografici, rendendo ancor più complessa la valutazione dell'intensità e della frequenza degli eventi estremi e del loro impatto sul territorio.

Per una pianificazione sostenibile, una gestione territoriale adeguata e una difesa efficace delle vite umane e dei beni privati e collettivi, è indispensabile conoscere meglio i rapporti fra il clima e le sue variazioni, la frequenza e l'intensità degli eventi meteo-idro-geologici estremi, il loro impatto sul territorio, gli ecosistemi, le risorse energetiche e le comunità, a diverse scale geografiche e temporali.

Il rischio vulcanico e la sua mitigazione sono temi che in Italia riguardano vasti centri urbani dell'area napoletana e siciliana e piccoli centri urbani insulari a forte pressione turistica. Lo studio dei fenomeni vulcanici, la previsione

dell'attività eruttiva attesa, la quantificazione del potenziale impatto, la catalogazione e la classificazione dell'esposto e la pianificazione di emergenza richiedono una "messa in scala" e un'integrazione delle operazioni tramite un approccio multidisciplinare con competenze che spaziano dalle geoscienze all'ingegneria, architettura, economia, statistica, sociologia, psicologia, comunicazione (così come suggerito anche all'interno del documento relativo all'articolazione 4). L'interazione tra vulcani, ambiente e uomo ha condizionato e condiziona fortemente la storia e lo sviluppo anche economico di intere aree in Italia e nel mondo; rappresenta un rischio relativamente raro, ma potenzialmente di grande impatto. In Italia, i dieci vulcani attivi hanno interagito profondamente con l'uomo fin da epoche molto remote. Nei periodi di quiescenza il vulcano rappresenta una risorsa per il territorio, per la natura fertile dei suoli, per la qualità delle acque e sorgenti termali a esso associate, per i paesaggi e le spiagge che lo caratterizzano. Viceversa, l'accadimento di eventi eruttivi può provocare desertificazione e inquinamento dei territori producendo danni ingenti al tessuto urbano, alle infrastrutture, alle reti di servizi, oltre a causare, nel caso di eventi estremi, perdita di vite umane e compromettere per periodi anche molto lunghi lo sviluppo socio-economico delle aree colpite. L'obiettivo principale di medio-lungo termine è quindi quello di sviluppare ricerche e conoscenze in grado di coniugare una sempre più efficace azione di mitigazione del rischio con lo sviluppo di un territorio resiliente e consapevole dei pericoli cui è esposto.

I georischi marini (frane sottomarine, tsunami, faglie attive, vulcanismo, emissioni di fluidi, migrazione di forme di fondo, flussi gravitativi) sono in grado di minacciare popolazioni e infrastrutture marine e costiere. Le attuali conoscenze hanno permesso di mappare la distribuzione degli elementi di pericolosità presenti sui fondali marini italiani, ma manca uno studio sistematico dei processi predisponenti e scatenanti gli eventi, così come la messa a punto di adeguati strumenti, piani di monitoraggio per la mitigazione del rischio.

Impatti

Impatto generale di tale articolazione è di migliorare la conoscenza dei processi fisici e degli eventi naturali responsabili di condizioni di rischio a tutte le scale spaziali e temporali, nel contesto dei cambiamenti climatici, ambientali e antropogenici in atto o previsti.

L'avanzamento della conoscenza e il miglioramento delle tecniche di monitoraggio (Articolazione 2) consentiranno lo sviluppo di modelli innovativi permettendo di riconoscere, individuare e cartografare le aree soggette a fenomeni di dissesto o disastro naturale, dalla scala locale a quella globale. Sarà quindi possibile fornire ai decisori soluzioni per interventi di mitigazione attraverso la riprogettazione del paesaggio rurale e urbano, e l'introduzione di prescrizioni urbanistiche e tecniche che riducano la vulnerabilità e in definitiva i rischi per la popolazione.

È di importanza critica che le ricerche pongano particolare attenzione all'incertezza di tali modelli. Solo con la conoscenza approfondita dell'incertezza delle previsioni si potrà ridurre il margine di errore dei modelli potenziandone l'utilità per le applicazioni pratiche a beneficio della sicurezza delle comunità. Ciò sarà possibile utilizzando un significativo numero di dati e osservazioni che permettano di sviluppare e combinare risultati derivanti da approcci fisicamente basati, di natura probabilistica e con tecniche di intelligenza artificiale.

SI favorirà quindi lo sviluppo di sistemi previsionali dei rischi naturali, sia per attuare le migliori pratiche di prevenzione, che per sviluppare sistemi "operativi" che consentano una risposta rapida al verificarsi di eventi estremi o improvvisi; sviluppare proiezioni degli eventi stessi in risposta ai cambiamenti globali in atto e attesi.

In tale contesto, la capacità di fornire in tempi brevi (secondi/minuti) scenari di possibile distribuzione spaziale dell'impatto sia diretto (nel caso di terremoti) che indiretto (fenomeni cosismici di liquefazione o frana) di un evento catastrofico è fondamentale e richiede lo sviluppo di modelli evoluti per la quantificazione di pericolosità, esposizione e vulnerabilità. Tale impatto è in linea con l'accordo delle Nazioni Unite per la riduzione del rischio a seguito di disastri (Sendai Framework 2015-2030), che ha portato alla creazione dell'International Network for Multi-Hazard Early Warning Systems all'interno della Global Platform for Disaster Risk Reduction.

Articolazione 2. Monitoraggio dei sistemi naturali

I dati e le informazioni sui sistemi naturali, derivanti dai sistemi di monitoraggio ambientale, sono fondamentali per un gran numero di applicazioni e servizi e costituiscono le piattaforme di base per le scelte programmatiche e strategiche finalizzate ad una migliore previsione, gestione e mitigazione dei rischi naturali e dell'impatto antropico anche in un contesto di cambiamenti globali. Il loro uso operativo richiede l'impiego di strumenti, protocolli e metodologie multidisciplinari e tecnologicamente avanzate che integrino, da un lato, le tecnologie di Osservazione della Terra da satellite e in situ, le reti-multi strumentali, i Sistemi di Supporto alle Decisioni e le piattaforme WebGIS operative per l'organizzazione, il trattamento e la divulgazione dei dati, secondo le direttive standard europee ed internazionali e, dall'altro, soddisfino le attuali esigenze del mondo della ricerca e dei servizi. La ricerca in tale settore, oltre che rispondere alle esigenze dirette all'acquisizione di dati innovativi tesi al monitoraggio e comprensione dei sistemi naturali, deve portare all'adozione di procedure standard e principi comuni alla comunità scientifica, agli utilizzatori ed alla loro condivisione.

Affrontare in modo unitario e organico il monitoraggio dei fenomeni naturali e la gestione efficace e razionale di megadati, è momento indispensabile di qualsiasi strategia di mitigazione dei rischi naturali soprattutto in un ambiente come quello del sistema Italia che comprende una varietà di situazioni geologiche dalle quali derivano pericolosità geo-idro-meteorologiche con magnitudo anche molto elevate. La produzione di dati sperimentali raccolti in modo sistematico e accurato in sito e in laboratorio è quindi fondamentale per la comprensione dei fenomeni di base e di quelli più complessi ed integrati che si verificano a livello territoriale.

In tale contesto rientra la realizzazione e l'implementazione di innovativi strumenti tecnologici che favoriscono la gestione integrata e interoperativa dei dati nelle fasi di previsione, prevenzione, monitoraggio, mitigazione dei rischi naturali, nonché degli impatti antropici. Tale gestione si realizza attraverso la progettazione e l'implementazione di sistemi per una rapida raccolta e condivisione delle informazioni disponibili (anche in corso d'evento) tra decisori, gestori del rischio e cittadini, favorendo anche soluzioni non-strutturali in cui il ″sensore umano″ gioca un ruolo di primaria importanza (Volunteered Geographic Information). Lo sviluppo ed uso dei Sistemi Informativi Territoriali è supporto indispensabile di tale gestione integrata e interoperativa dei dati ambientali ottenuti con i diversi sistemi di Osservazione della Terra, o prodotti dall'applicazione di modelli statistici, deterministici o fisicamente basati, o derivanti da reti di laboratori e piattaforme tecnologiche per il processamento dei dati ambientali a supporto dell'analisi della pericolosità, dei rischi e degli impatti legati ad attività antropica. Per questo la progettazione e l'implementazione di Sistemi Informativi Modulari di Supporto alle Decisioni è fondamentale per fornire ai pianificatori territoriali e ai gestori dell'emergenza un valido supporto al processo decisionale, sfruttando nuove tecnologie e strategie innovative e con il completo recepimento del quadro normativo vigente a livello regionale, nazionale ed europeo. Per quanto riguarda gli impatti antropici risulta prioritario lo sviluppo e l'applicazione di nuove tecnologie sostenibili rivolte alla mitigazione del rischio indotto da emissioni in atmosfera e rilasci incontrollati nelle matrici ambientali.

Obiettivi

L'obiettivo generale è quello di identificare le caratteristiche peculiari di una infrastruttura di dati ambientali, di tipo Open-Access, da essere progettata ed implementata in modo modulare, interoperabile e distribuita ed in grado di promuovere l'archiviazione, l'acquisizione anche in near real time, la gestione, l'analisi e la comunicazione/disseminazione di dati ambientali, a supporto delle azioni di conoscenza, previsione, prevenzione, monitoraggio, gestione e mitigazione dei rischi naturali e degli impatti antropici. In tale contesto, il raggiungimento di tale obiettivo potrà concretizzarsi sulla base degli elementi elencati nel seguito.

- ✓ Lo sviluppo ed utilizzo delle più avanzate tecnologie per le misure sperimentali, le osservazioni in campo e da satellite per il monitoraggio dei fenomeni naturali o indotti dall'uomo che si interfacciano con i servizi Copernicus e che costituiscono gli elementi per la progettazione di infrastrutture operative di gestione per la sicurezza dei sistemi naturali, impatti antropici (includendo anche il patrimonio dei beni culturali e l'inquinamento delle matrici ambientali), e dove l'organizzazione, trattamento e divulgazione dei dati è in

accordo alle direttive standard europee ed internazionali. Queste infrastrutture sono quindi strettamente connesse alle altre macrotematiche e da esse anche "alimentate".

- ✓ La promozione dell'interdisciplinarità per la ricerca e l'innovazione tecnologica per rispondere alle esigenze di acquisizione di dati innovativi per il monitoraggio e la comprensione dei sistemi naturali, che si concretizza con l'adozione di procedure standard utili alla comunità scientifica, ai fruitori ed alla loro condivisione (TRL atteso: 4 - 9).
- ✓ La creazione di reti di eccellenza scientifica multidisciplinari fra Enti di Ricerca ed Università, che consentono di fornire modelli e soluzioni tecnologiche avanzate ed economicamente sostenibili per la previsione, prevenzione, protezione e mitigazione dei rischi, nonché per la riduzione degli impatti delle pressioni antropiche sull'ambiente, creando le condizioni per una società sempre più sostenibile e resiliente.

Pertanto, la declinazione degli obiettivi specifici risulterà nell'insieme degli obiettivi prioritari elencati in seguito.

1. Contribuire a rafforzare in modo sinergico lo sviluppo ed il potenziamento di un sistema integrato di laboratori ed infrastrutture di ricerca con riferimento a:
   - Tecniche, prodotti e dispositivi per l'analisi e valutazione dei rischi naturali e degli altri rischi ambientali
   - Dispositivi, sensori e soluzioni per la protezione del territorio.
   - Sistemi di allerta precoce (early warning) e gestione dell'emergenza legata ai rischi ambientali.
   - Nuove tecnologie per ridurre l'impatto degli eventi naturali e dell'azione antropica sull'ambiente.
2. Consolidare e approfondire le attività di ricerca nel settore ambientale, sviluppando le iniziative già avviate, individuando nuovi itinerari di ricerca e potenziando il trasferimento tecnologico e delle conoscenze per l'erogazione di servizi scientifici e tecnologici dedicati al monitoraggio, al controllo e alla tutela dell'ambiente.
3. Razionalizzare e rendere più efficiente la rete delle infrastrutture di ricerca nazionali che possano costituire un punto di riferimento per la Protezione Civile, per enti di ricerca anche internazionali ed Aziende per tutte le problematiche ambientali. Lo sviluppo di una rete di servizi di monitoraggio e di modellazione, sia del territorio sia dei singoli eventi associati ai rischi naturali ed alle problematiche di impatto ambientale e di inquinamento connesse ai rischi antropici renderà più efficace l'azione di mitigazione dei rischi ed il loro impatto anche sull'ecosistema, con particolare riferimento alla tutela delle risorse ambientali e culturali e delle specificità del territorio.

Impatti

Impatti attesi includono gli elementi chiave elencati nel seguito.

1. Avanzamento nello sviluppo ed implementazione di sensori, strumenti e reti di monitoraggio, in particolare multiparametriche, anche con riferimento alla standardizzazione delle tipologie di monitoraggio e alla valutazione di impatti antropici. Questo riguarderà l'utilizzo e la condivisione (anche attraverso piattaforme WebGIS) di informazioni strategiche (esistenti o da sensori terrestri, aerotrasportati e/o da satellite), in tempo quasi reale, e di tecniche di modellazione per costruire nuove mappe o aggiornare periodicamente mappe esistenti di suscettibilità, di pericolosità e di impatto antropico riconoscendo il ruolo centrale dello sviluppo ed utilizzo di tecnologia avanzata nelle strategie di previsione, prevenzione, monitoraggio e mitigazione dei rischi e degli impatti antropici sulle matrici ambientali, sinergicamente integrati con i servizi di soccorso e difesa civile.
2. Sviluppo e potenziamento di infrastrutture sperimentali in sito e in laboratorio a supporto delle azioni di conoscenza, previsione, prevenzione, monitoraggio, gestione e mitigazione dei rischi naturali e degli impatti antropici (in ambiente terrestre e marino). Ciò si traduce in azioni di rafforzamento della dotazione tecnologica e funzionale delle infrastrutture esistenti e nella creazione di nuove infrastrutture competitive a livello europeo capaci di fornire nuovi dati in base ai quali aumentare le conoscenze di base necessarie per lo sviluppo di modelli previsionali attendibili. È necessario uno sforzo volto sia al potenziamento delle strutture e delle tecniche di osservazione sia alla piena e organica integrazione dei dati provenienti dalle numerose metodologie di indagine di tipo geofisico, geochimico e geologico disponibili. Particolare attenzione merita, il monitoraggio in ambiente marino, settore tematico in forte avanzamento in varie aree al mondo (es. Giappone). In questo settore sono evidenti i limiti conoscitivi connessi con la scarsità di dati disponibili e la carenza di navi oceanografiche che pone

la comunità scientifica nazionale in difficoltà rispetto alle altre comunità internazionali. Inoltre, il potenziamento delle infrastrutture di ricerca svolge un ruolo fondamentale nell'avanzamento della conoscenza di base e nello sviluppo dell'innovazione e delle sue possibili applicazioni anche a fini economici ed occupazionali. Per la mitigazione dei rischi sismico e vulcanico, è necessario disporre di nuove reti di monitoraggio ed osservative integrate, anche tramite le più avanzate tecnologie ICT che consentano un miglioramento delle conoscenze sulla fisica delle sorgenti e la propagazione delle onde sismiche, sull'innesco e la dinamica delle eruzioni e sul miglioramento delle capacità previsionali dei rischi geo-idrologici considerando la non stazionarietà delle forzanti dovuta ai cambiamenti climatici. L'evolversi della pressione antropica sul territorio ha determinato l'alterazione e spesso il rischio inquinamento delle matrici ambientali ed è vitale sviluppare una rete di monitoraggi che tuteli le risorse naturali e paesaggistiche ed i Beni culturali di cui il nostro paese è ricco. Tali infrastrutture dovranno essere costituite da un sistema di archivi e portali, che raccolgono ed integrano i dati ambientali e li rendono disponibili in un'ottica *open access*, permettendo la loro distribuzione e disseminazione e favorendo di fatto lo sviluppo e l'applicabilità di tecnologie osservative e metodologie di analisi della complessa dinamica dei processi alla base dei rischi naturali e dei fattori chiave ambientali che ne sono la causa innescante e nonché degli impatti antropici in ambienti fisiografici differenti.

3. Implementazione e creazione di banche dati ad elevato contenuto informativo, spaziale e temporale, adeguate a sostenere monitoraggi e modellazioni multi-scala. Per questo è fondamentale lo sviluppo e trasferimento tecnologico di piattaforme WebGis che favoriscono la gestione integrata ed interoperativa di banche dati ambientali al suolo e/o da satellite sviluppate con la finalità di consentire servizi di mappatura/monitoraggio delle aree impattate da fenomeni naturali e da azioni antropogeniche e di rendere disponibili i nuovi dati acquisiti a sistemi di modellazione dedicati per differenti tipologie d'evento. Le piattaforme devono avere la peculiarità di essere "modulari" e "trasversali" a tutte le tipologie di rischio e di impatto antropico cui i sistemi naturali sono soggetti, mediante anche l'accesso aperto ai dati e ai risultati scientifici e tecnologici raggiunti
4. Sviluppo di metodologie efficienti per l'analisi e la gestione operativa e razionale di grandi data base ad accessibilità pubblica. La realizzazione dei data base favorirà la comunicazione/disseminazione dei dati e dei risultati verso la comunità scientifica ma anche verso la società civile fornendo in tal modo una chiara visione sulle problematiche connesse ai rischi naturali, agli impatti antropici e alla tutela ambientale in termini di dati, eventi, risultati della ricerca, misure di mitigazione e buone pratiche di adattamento ai cambiamenti globali. Questo aspetto è in accordo al fondamentale ruolo della Terza Missione della Ricerca che è finalizzata a trasmettere all'industria ed alla società civile il trasferimento tecnologico e tutte le nuove conoscenze sui potenziali rischi a cui sono sottoposti i sistemi naturali e nonché agli impatti sulle matrici ambientali a seguito di azioni antropiche.
5. Integrazione di piattaforme open access per dataset, risultati scientifici e tecnologici utilizzabili in condivisione con la società civile e come strumento operativo per la governance del multi-rischio e degli impatti antropici. Le infrastrutture favoriranno la comunicazione/disseminazione dei dati e dei risultati verso la comunità scientifica ma anche, attraverso sezioni dedicate, verso la società civile fornendo in tal modo una chiara visione sulle problematiche connesse alla sicurezza dei sistemi naturali e agli impatti antropici in termini di dati, eventi, risultati della ricerca, misure di mitigazione e buone pratiche di adattamento ai cambiamenti globali. L'infrastruttura, modulare e interoperabile, funzionerà come supporto "trasversale" a tutte le tipologie di rischio e consentirà l'accesso aperto ai dati e ai risultati scientifici e tecnologici raggiunti.

Articolazione 3. Strategie multi-rischio per la difesa da eventi naturali

Gli eventi naturali (come terremoti, frane, inondazioni, incendi, uragani, tsunami, valanghe) e di origine antropica possono causare danni ingenti e perturbazioni sociali ed economiche. Molti di questi eventi sono interdipendenti (ovvero gli uni possono causare gli altri) e/o possono verificarsi sia contemporaneamente che in stretta successione (eventi a cascata). Ciò porta ad effetti talvolta enormi sul complesso sistema costituito dall'ambiente naturale, popolazione, beni, strutture ed infrastrutture, attività umane, economia, servizi di un'intera nazione o più nazioni coinvolte.

Questi eventi non sono mai completamente evitabili, ma spesso possono essere mitigati o anticipati tramite la comprensione dei fenomeni e delle loro interdipendenze ed una migliore conoscenza del territorio, che consentono

l'allocazione delle risorse necessarie per una efficiente mitigazione del rischio, sia tramite azioni di preparazione e prevenzione, che di facilitazione di un recupero rapido dopo l'accadimento dell'evento.

Tali azioni possono includere l'abbandono o l'adeguamento di strutture vulnerabili esistenti, il miglioramento dei codici di costruzione e/o della pianificazione dell'utilizzo del territorio avendo piena coscienza dei rischi esistenti, dell'impiego di risorse finanziarie come strumenti per il trasferimento di perdite ed il finanziamento delle fasi post-disastro.

Un'attenta valutazione dei rischi e della sovrapposizione dei loro effetti è alla base di una programmazione ottimale, che consente di prepararsi adeguatamente a potenziali accadimenti futuri, facilitando i decisori ad esprimere giudizi, definire priorità ed intraprendere azioni sulla base di informazioni robuste e tenendo conto adeguatamente delle incertezze anche nelle pressanti condizioni post- evento.

Per raggiungere questo obiettivo è necessaria un'attenta valutazione dei rischi attesi e potenzialmente disastrosi a cui una comunità può essere esposta, attraverso una migliore comprensione e modellazione dei processi fisici e delle loro possibili sovrapposizioni, nonché una conoscenza approfondita della risposta manifestata in occasione di precedenti eventi. Di particolare interesse sono sia la risposta della comunità nel suo insieme che dei suoi singoli individui, nonché le potenziali conseguenze socio-economiche.

Negli approcci in cui gli rischi vengono trattati separatamente (single type risk assessment) è necessario lo sviluppo e l'affinamento di metodologie "ad hoc" per il confronto dei risultati tenendo conto delle diverse incertezze e scale spaziali e temporali degli eventi naturali. Simili problematiche meritano attenzione anche nelle stime multi-rischio, laddove lo sviluppo di curve di fragilità multi-parametriche e l'analisi sia relativa a stime probabilistiche adatte alla pianificazione territoriale, che allo sviluppo di scenari di interesse per la mitigazione del rischio in fase post- evento risultano ancora essere in una fase iniziale di elaborazione.

Queste problematiche appaiono di particolare rilevanza per un paese come l'Italia, una delle nazioni più esposte ai rischi naturali, per la cui riduzione è opportuno sviluppare metodologie e sistemi finalizzati alla previsione, valutazione e mitigazione degli effetti potenzialmente dannosi. Questi studi devono essere affiancati da ricerche di base in grado di migliorare le capacità previsionali dei fenomeni (es. sismici, vulcanici, geomorfologici, di frana, meteorologici), da studi sui precursori, dall'aggiornamento/completamento di dataset e dalla loro implementazione in sistemi informativi territoriali, anche utilizzando sistemi di osservazione integrati, in modo da facilitare lo sviluppo ed implementazione di approcci per la valutazione quantitativa della pericolosità e del rischio, in un contesto multi-hazard.

Per garantire la definizione di scenari di pericolosità e rischio affidabili e completi occorre integrare competenze di base multi- ed inter-disciplinari. È necessario giungere ad un efficace e sistematico utilizzo delle conoscenze scientifiche e tecnologiche nelle strategie multilivello di mitigazione e prevenzione dei rischi naturali (in ambiente terrestre e marino) e degli impatti indotti da attività antropiche sulle matrici ambientali.

La quantificazione degli impatti antropici a diverse scale spazio-temporali pone nuove sfide nella prevenzione e gestione degli eventi e delle catastrofi naturali e indotte da azioni antropogeniche e si configura come elemento chiave per una valutazione complessiva e robusta del rischio associato, anche alla tutela dei beni culturali e paesaggistici.

Per raggiungere tali finalità occorre sviluppare: a) tecniche di raccolta dati ad elevata risoluzione ed a scale confrontabili per l'analisi dei diversi rischi con dettaglio confrontabile, con data policy condivise; b) l'integrazione di tecnologie e sistemi di monitoraggio, in-situ e da remoto; c) sistemi e strumenti per l'elaborazione e la modellazione di dati e informazioni multi-parametriche, includendo lo sviluppo e la sperimentazione di tecnologia avanzata per sistemi di early warning multi-rischio dei fenomeni naturali; d) tecniche di data analysis applicate a big data; e) sistemi e strumenti per l'individuazione di possibili condizioni di criticità dei sistemi naturali e di strutture ed infrastrutture con essi interagenti, con particolare attenzione alla funzionalità delle reti di comunicazione e degli edifici strategici; f) metodologie per una valutazione quantitativa robusta ed affidabile del multi-rischio, per l'aggiornamento delle valutazioni e per generare proiezioni in funzione di diversi scenari (es. variazioni climatiche, uso del suolo).

La ricerca è mirata ad identificare elementi utili per la governance e la gestione dei rischi ed a dare la necessaria rilevanza alla prevenzione ed alla riduzione della vulnerabilità, nonché all'aumento della capacità di risposta e della

resilienza. Sviluppi significativi di conoscenze e tecnologie consentiranno valutazioni appropriate ed affidabili di scenari, quantificandone pericolosità, livelli di esposizione e vulnerabilità, alle differenti scale spaziali e temporali che caratterizzano i diversi eventi naturali ed indotti dall'uomo, migliorando la quantificazione e la comunicazione dei risultati ottenuti nella stima della pericolosità e del rischio e della relativa incertezza.

In tale contesto, la capacità di fornire in tempi brevi scenari di possibile distribuzione spaziale dell'impatto sia diretto (nel caso ad esempio di terremoti), che indiretto (ad esempio, fenomeni cosismici di liquefazione o frana) di un evento catastrofico è fondamentale e richiede lo sviluppo di modelli evoluti per la quantificazione di pericolosità, esposizione e vulnerabilità.

Obiettivi

Gli obiettivi che prioritariamente si prevede di perseguire riguardano principalmente il miglioramento delle valutazioni quantitative degli eventi e dei loro impatti, alle diverse scale geografiche e temporali, nel contesto dei cambiamenti globali in atto e/o previsti.

Tali obiettivi vanno raggiunti attraverso attività sinergiche e multi-disciplinari che mirano a produrre avanzamenti nelle capacità di: a) definire la pericolosità per i diversi fenomeni, dalla scala locale a quella globale, includendo l'analisi multi-hazard e multi-risk, individuando hotspot per concentrazione di più rischi e/o per livello di rischio; b) sviluppare sistemi previsionali che consentano modellazioni affidabili pre- evento, la pianificazione di azioni di mitigazione ed eventualmente una risposta rapida al verificarsi degli eventi naturali o indotti da azioni antropogeniche; c) produrre modelli previsionali degli eventi e/o dei loro impatti, con particolare attenzione alla stima del rischio per la popolazione, per le strutture ed infrastrutture strategiche; d) definire nuovi criteri e metodi per la tempestiva ricognizione dello stato e del livello di evoluzione dei fenomeni naturali in atto e dei danni post-evento, favorendo la comprensione e previsione della risposta del sistema naturale, ed il rapido ripristino dei livelli di sicurezza; e) fornire soluzioni di mitigazione dei rischi attraverso interventi che riducano la pericolosità, l'esposizione e la vulnerabilità, aumentando la capacità di risposta e la resilienza della popolazione, dei beni economici ed infrastrutturali, dei beni culturali e dei capitali naturali.

Impatti

Questa articolazione si propone di sviluppare attività di ricerca e innovazione tecnologica finalizzate all'implementazione di metodologie e sistemi per la valutazione quantitativa degli effetti di scenari multi-hazard e multi-rischio per la previsione (early warning), l'allertamento e la valutazione degli impatti indotti da eventi potenzialmente dannosi. In particolare, sono previsti avanzamenti nelle capacità di:

1. Favorire approcci avanzati multi-hazard e multi-risk a varie scale spaziali e temporali (long-term and short-term assessment) in grado di individuare aree e livelli di esposizione ai rischi, integrare misure strutturali e non strutturali per la mitigazione e prevenzione dei rischi naturali e degli impatti antropici.
2. Favorire lo sviluppo dei sistemi conoscitivi e valutativi della esposizione, della vulnerabilità e resilienza della popolazione, dei beni economici, strutturali e infrastrutturali, dei beni culturali e dei capitali naturali.
3. Migliorare le capacità di valutazione e stima degli impatti antropici sulla resilienza dei sistemi naturali anche ai fini dell'adattamento ai cambiamenti globali.
4. Individuare nuovi criteri e metodi per la tempestiva ricognizione dello stato e del livello di evoluzione dei fenomeni naturali in atto e dei danni post- evento, per l'aggiornamento degli scenari di rischio e per favorire il pronto ripristino dei livelli di stabilità e sicurezza dei sistemi naturali.

Articolazione 4. Governance e gestione dei rischi naturali e degli impatti antropici

La governance del rischio associato ad eventi naturali richiede di valutare e affrontare diverse tipologie di conseguenze possibili o probabili, tra cui le perdite di vite umane e i danni alla salute, alle strutture e infrastrutture, alla società e all'economia, nonché agli ecosistemi. Attualmente, tale governance si realizza in presenza di importanti

cambiamenti climatici e globali, ed è quindi indispensabile che le strategie e i piani di riduzione dei rischi, di gestione e di sviluppo del territorio tengano conto di tutte quelle variazioni dei sistemi naturali che, siano esse proprie o indotte dalle attività umane, possono avere conseguenze importanti a diverse scale spaziali e temporali. La capacità di sviluppare una governance robusta ed efficiente richiede quindi la necessità di comporre un'ampia gamma di conoscenze e capacità a livello scientifico, professionale, gestionale, istituzionale e politico.

L'Italia presenta un sistema molto articolato di attori, anche del sistema ricerca-innovazione, e di processi istituzionali rivolti alla valutazione e gestione a dei rischi naturali. Questa condizione riflette l'elevata densità, intensità e varietà dei rischi a cui il Paese è soggetto e la molteplicità dei livelli di governo coinvolti, dallo Stato alle regioni, fino alle le amministrazioni comunali e ai diversi organismi di governo del territorio (ad esempio le Autorità di Bacino) che operano con un ampio insieme di strumenti, più o meno standardizzati, di programmazione a base tecnica. Esempio di tale articolazione è lo stesso sistema di Protezione Civile che, seppure in modo gerarchico e proceduralmente definito, coinvolge una pluralità di attori attivi, compresi quelli del sistema scienza/ricerca, nella caratterizzazione ex ante dei rischi, nella loro gestione, e nella risposta agli eventi. Più in generale, il sistema di governance dei rischi naturali combina un uso esteso, intensivo, sistematico e permanente di supporti di conoscenza scientifica, siano essi dedicati o generali, con processi di bilanciamento degli interessi dei diversi stakeholder sociali, economici ed istituzionali. Questi stessi stakeholder sono, attraverso le loro azioni, possibili agenti antropici del rischio e, nel contempo, potenziali vittime del rischio stesso quando si materializza in eventi.

Tale combinazione tra elevata densità tecnico-scientifica e complessità delle politiche pubbliche determina una gamma ampia, differenziata ed eterogenea di fabbisogni conoscitivi, che vanno dall'uso routinario di 'scienza normale' ad un continuo flusso di nuove domande di ricerca che richiedono scienza di frontiera, sia essa fondamentale o applicata. Allo stesso tempo, richiede una significativa capacità di trasferimento e traduzione della conoscenza scientifica in strategie operative efficaci di minimizzazione e gestione dei rischi e dei loro effetti potenziali.

Obiettivi

Obiettivo generale è lo sviluppo di ricerca multidisciplinare per la messa a punto di modelli e strumenti informativi, conoscitivi, decisionali e procedurali utili alla definizione di strategie integrate e partecipative di prevenzione, mitigazione e gestione dei rischi e degli impatti generati da attività antropica.

A tal fine, vanno perseguiti:

- Una più ampia visione della ricerca sul rischio in cui si compenetrano la sicurezza dei sistemi naturali e la sicurezza dei sistemi sociali.
- Un ampliamento della gamma delle discipline scientifiche che fanno ricerca sui temi dei rischi naturali nella loro interazione con l'azione antropica, superando, in particolare, l'attuale circoscritto interesse da parte dell'ampio sistema delle scienze umanistiche, sociali, politiche, giuridiche ed economiche. Tali discipline possono positivamente contribuire ad una più piena conoscenza di come gli hazard naturali possono tradursi in rischi attraverso le attività umane, i comportamenti, gli assetti organizzativi, e di come gli eventi naturali si traducono in perdite umane e materiali.
- Lo sviluppo di originali modellistiche multidisciplinari in cui le conoscenze sulle dinamiche fisiche ed ecologiche dei sistemi naturali prodotte dalle scienze della terra e dalle altre scienze applicate ai rischi, vengono direttamente integrate con le corrispondenti variabili e dimensioni antropiche, sia come fattori non fisici di esposizione e vulnerabilità sia come misure di potenziale resilienza di persone, comunità e organizzazioni agli eventi naturali. Tale modellistica integrata può fornire strumenti più avanzati efficaci al sistema multilivello di governance del rischio
- La creazione di sistemi informativi ad elevato dettaglio territoriale sulle esposizioni che, oltre a quelle fisiche, comprendano anche le esposizioni economiche (es. strutture produttive, reti di fornitura inter-industriale, reti di mobilità del lavoro), le esposizioni di beni culturali, che nel nostro Paese presentano una densità e un valore che non ha confronti, i siti ad alta criticità e vulnerabilità sociale (es. scuole, luoghi di cura), i nodi critici delle reti infrastrutturali fisiche e non fisiche. Tali sistemi informativi possono supportare lo sviluppo

della modellistica 'aumentata' con le dimensioni sociali e costituire un nodo centrale nella definizione di strategie di soccorso e protezione civile e piani di intervento emergenziali.

- Lo sviluppo di ricerca integrata di base e multidisciplinare sulla vulnerabilità che, oltre alla dimensione fisica e tecnico-ingegneristica, comprenda le vulnerabilità sociali e organizzative delle comunità esposte. Si tratta di elementi soggetti a crescenti possibilità di misurazione che risultano di grande importanza per strategie di mitigazione e prevenzione non generiche e ad alta priorità per le situazioni di alta vulnerabilità. In linea con la ricerca internazionale, è opportuno un ampliamento di prospettiva che colloca la vulnerabilità nell'ambito dei più ampi concetti e misure di resilienza, anche in questo caso integrata tra fenomeni fisici e fenomeni sociali, organizzativi e tecnologici.
- Un aumento del coinvolgimento dei cittadini nei processi di ricerca sul rischio attraverso pratiche di 'citizen science', così da aumentare ulteriormente il loro ruolo decisivo sia nella prevenzione che nella gestione dei rischi, oltreché nelle situazioni di emergenza e ricostruzione post-evento.

Impatti

Impatti attesi includono gli elementi chiave elencati nel seguito.

1. Migliore utilizzo di moderne conoscenze scientifiche e tecnologiche nella gestione e governance dei rischi e degli impatti antropici, e riduzione del gap conoscitivo tra policy makers e comunità professionale e scientifica. La flessibilità e interoperabilità delle reti digitali offre una crescente possibilità di accesso aperto alle reti informative delle diverse amministrazioni pubbliche e ai database resi disponibili nella rete dagli organismi del sistema della ricerca e dai singoli ricercatori (open data di pubblicazioni). Una maggiore integrazione di conoscenze socio-economiche può consentire un migliore dialogo tra ricerca scientifica e decisioni amministrative, organizzative e di programmazione per la prevenzione e la gestione dei rischi. Può inoltre contribuire a comprendere l'attitudine ad assumere o evitare rischi da parte delle persone e delle organizzazioni, che costituisce un elemento chiave per impostare strategie di prevenzione e mitigazione.
2. Metodologie robuste per la valutazione integrata dei costi multipli, diretti ed indiretti, associati a disastri naturali e indotti da attività antropica e dei benefici netti di investimenti in prevenzione/mitigazione. Lo sviluppo di modellistiche integrate multidisciplinari può fornire scenari più completi degli effetti indiretti, indotti e concatenati, più realistiche valutazioni del valore degli investimenti pubblici in prevenzione e mitigazione dei rischi, strumentazioni più robuste per incorporare i rischi nelle decisioni pubbliche di gestione del territorio, valutazioni più credibili dei costi, pubblici e privati, degli eventi naturali, e migliori è più convincenti conoscenze di supporto alle strategie di coinvolgimento dei cittadini.
3. Sviluppo di strumenti per la pianificazione e gestione del rischio con forte enfasi sulla riduzione di esposizione e vulnerabilità e l'aumento della resilienza, fino alla definizione e selezione delle più appropriate tipologie di intervento tecnico. La ricerca integrata multidisciplinare sulle dimensioni e la misurazione della vulnerabilità e resilienza dei sistemi complessi apre nuove possibilità di ricerca predittiva e di scenarizzazione che può essere di particolare importanza nell'orientare le scelte pubbliche di protezione, soccorso e difesa dei cittadini.
4. Strategie condivise e partecipate di riduzione dei rischi in sistemi fortemente antropizzati, nell'ambito dei processi di 'città intelligente' e adattamento a mutazioni climatiche, anche con riferimento ad aree costiere e ad aree ad alta fruibilità turistica e alto valore artistico culturale.
5. Strategie di coinvolgimento dei cittadini e delle comunità come alleati attivi delle strategie contro i rischi naturali. I processi di coinvolgimento, anche attraverso pratiche di citizen science, possono utilmente contribuire ad orientare le priorità e, nel contempo, creare consapevolezza individuale e collettiva dei rischi e delle possibilità di loro mitigazione attraverso pratiche quotidiane collaborative e azioni di autotutela. Le metodologie e le prassi di coinvolgimento, anche basate sui social media, rappresenta un campo di ricerca crescente che ha ampie possibilità di integrazione soprattutto con la ricerca applicata sui rischi naturali e quella a supporto delle decisioni pubbliche. È inoltre auspicabile lo sviluppo di procedure e applicazioni che possano sfruttare, anche a fini di ricerca, i dati osservativi prodotti, in modo sempre più intenso, direttamente dai cittadini.

6. Lo sviluppo della ricerca e della modellistica multidisciplinare può fornire supporto conoscitivo allo sviluppo di nuovi schemi finanziario-assicurativi per la copertura dei rischi naturali che intervengano a complemento del ruolo centrale, e non surrogabile, dello Stato nella protezione dei cittadini. Tale impatto atteso è coerente con lo sviluppo in atto di strategie dell'Unione Europea per la promozione e regolazione della 'finanza sostenibile', e con la tendenza ormai affermata ad includere il rischio climatico tra le componenti di valutazione della rischiosità degli investimenti pubblici e privati.

Interconnessioni con altri ambiti tematici

La mitigazione dei rischi è un obiettivo strategico per il presente e per il futuro del nostro paese che è strettamente interconnessa con la tutela ambientale e la conservazione delle risorse del pianeta Terra. La sfida ambientale rappresenta un tema non più eludibile per le future generazioni ed impone una visione unitaria dei sistemi naturali ed un approccio fortemente interdisciplinare. È prioritario quindi valorizzare e mettere a sistema le numerose eccellenze presenti nel paese costruendo insieme nuovi modelli di gestione del territorio e delle sue risorse. L'ambito tematico Sicurezza Sistemi Naturali ha quindi forti interconnessioni con tutti gli ambiti tematici che riguardano l'ambiente e le risorse ed i cambiamenti climatici. Inoltre, gli impatti ambientali e la loro mitigazione si trasmettono direttamente all'economia reale e al sistema finanziario. Il territorio italiano è particolarmente esposto ai rischi naturali (vulcani, terremoti ecc.) ed ai cambiamenti climatici per la sua natura geologica, l'idrografia, la configurazione geo-morfologica e l'estensione della linea di costa. Nello stesso tempo il territorio italiano ha un patrimonio di risorse naturali, paesaggistiche e culturali unico al mondo. È quindi necessario adottare una visione olistica e interdisciplinare per creare le condizioni di una società più resiliente, capace di affrontare le sfide future e cogliere le occasioni di sviluppo.

Ambito: Risorse agroalimentari e forestali

Il tema principale del gruppo di lavoro risorse agroalimentari è stato focalizzato sulla necessità di aumentare il cibo prodotto nei prossimi decenni in modo sostenibile, anche considerando scenari futuri di cambiamenti globali. Sinergie associate alle articolazioni del gruppo di lavoro Sicurezza Sistemi Naturali sono associabili agli elementi chiave dell'Articolazione 4, con particolare riferimento alle tematiche di governo del territorio e del ruolo che i rischi naturali possono avere sulla produzione alimentare (desertificazione delle regioni meridionali, eventi estremi, erosione e perdita di suolo). Rilevanti possono anche essere interazioni con l'Articolazione 2, con riferimento alla finalità di reti di monitoraggio multiparametriche per la valutazione (attraverso monitoraggio e assimilazione in modelli previsionali) di qualità e quantità di acqua e matrici ambientali, nonché con riferimento alla tutela di suoli da eventi di inquinamento e/o degrado.

Ambito: Gestione delle risorse marine

Il gruppo di lavoro sulla gestione delle risorse marine ha avuto come principale tema conduttore la necessità di avere nuove tecnologie per ridisegnare le attività economiche che insistono (direttamente o indirettamente) sull'ambiente marino, incluse le fonti di inquinamento. Articolazioni comuni con il gruppo di lavoro Sicurezza Sistemi Naturali includono l'Articolazione 1 (e.g., incremento della conoscenza di base dei processi che governano erosione costiera), nonché le Articolazioni 2 e 3 (e.g., utilizzo multifunzionale di reti di monitoraggio e l'utilizzo di tecniche di intelligenza artificiale per l'analisi e interpretazione di dati). Elementi di social acceptance inclusi nell'Articolazione 4 possono inoltre essere di interesse reciproco ai due tavoli.

Ambito: Trasformazioni sociali, società dell'inclusione

Il gruppo di lavoro sulle trasformazioni sociali e società dell'inclusione ha avuto tra i suoi temi di maggior interesse l'impatto che le principali trasformazioni sociali, inclusa l'innovazione tecnologica e la digitalizzazione possono avere su aspetti che governano la qualità della vita. Di conseguenza, punti di maggiore sinergia con il gruppo di lavoro Sicurezza Sistemi Naturali posso essere legati alle attività previste nell'Articolazione 4, in cui le tematiche dell'inclusione sociale a vari livelli sono affrontate, anche con riferimento allo sviluppo di un modello di governance partecipato a vari livelli (includendo aspetti di ricerca e innovazione tecnologica).

Ambito: Cambiamenti climatici e adattamento

Il gruppo di lavoro sul cambiamento climatico affronta il tema degli impatti dell'evoluzione del clima sui sistemi fisici, naturali, agricoli, urbani, sociali, economici e della salute. Il collegamento con le attività del gruppo di lavoro Sicurezza Sistemi Naturali è riferibile alle Articolazioni 1, 2 e 3. In tali contesti, si affronta lo sviluppo di modelli previsionali, metodi di stima del rischio e misure di monitoraggio della risposta del sistema a diverse sollecitazioni di tipo ambientale, inclusi i cambiamenti globali. Una collaborazione tra i due ambiti di ricerca sembra quindi auspicabile.

Ambito: Intelligenza artificiale

Il gruppo di lavoro sull'Intelligenza Artificiale (AI) affronta il tema della ricerca di base, includendo possibili applicazioni alle sfide sociali e dell'ambiente. Il collegamento con le attività del gruppo di lavoro Sicurezza Sistemi Naturali è in particolare sui temi inclusi nell'Articolazione 1 e 2. Si auspica una collaborazione fra i due ambiti di ricerca, con particolare riferimento alla possibilità di prevedere lo sviluppo di ambienti computazionali in grado di integrare i diversi elementi che governano i processi evolutivi dei sistemi naturali, anche favorendo la sinergia tra tecniche probabilistiche, approcci fisicamente basati e tecniche di intelligenza artificiale. Si auspica inoltre una sinergia nello sviluppo di metodologie efficienti per l'analisi e la gestione operativa e razionale di grandi data base ad accessibilità pubblica.

Ambito: Sicurezza delle strutture, infrastrutture e reti

Il gruppo di lavoro sulla Sicurezza delle strutture, infrastrutture e reti affronta il tema ampio della sicurezza e resilienza dell'ambiente costruito e delle infrastrutture considerando aspetti legati a vulnerabilità dei sistemi, molteplicità dei pericoli di origine naturale e antropica nonché conoscenza imperfetta e/o incompleta di eventi pericolosi e dei loro impatti. La collaborazione con le attività del gruppo di lavoro Sicurezza Sistemi Naturali è auspicabile sulla gran parte delle tematiche associate alle Articolazioni previste.

Ambito: Transizione digitale

Il gruppo di lavoro sulla Transizione Digitale affronta il tema di mettere a sistema e valorizzare pienamente il potenziale dell'innovazione digitale a vantaggio delle diverse esigenze e prospettive che possono emergere a livello individuale, di comunità e del Sistema Paese, con particolare riferimento anche alla gestione della pandemia COVID19. Il collegamento con l'attività del gruppo di lavoro Sicurezza Sistemi Naturali è molto ampio per il ruolo fondamentale delle tecnologie digitali, anche a supporto dell'uso di una ampia varietà di altre tecnologie, ed è principalmente associabile ai temi delle Articolazioni 2 e 3, con particolare riferimento allo sviluppo di metodologie efficienti per l'analisi e la gestione operativa e razionale di grandi data base ad accessibilità pubblica, all'integrazione di piattaforme open access per dataset e/o allo sviluppo di metodologie e sistemi per la valutazione quantitativa degli effetti di scenari multi-hazard e multi-rischio.

Ambito: Cybersecurity

Il gruppo di lavoro sulla Cybersecurity affronta il tema di identificazione delle minacce cibernetiche e dello sviluppo di soluzioni avanzate per la protezione e il recupero da possibili attacchi informatici alle reti di distribuzione, alle infrastrutture e alle specifiche tecnologie a supporto dell'erogazione di servizi essenziali, inclusi i servizi sanitari e socio-sanitari. Il collegamento con il gruppo di lavoro Sicurezza Sistemi Naturali è molto trasversale alle diverse articolazioni proposte in quanto tutte le diverse tecnologie per la salute dovranno essere oggetto di attenzione di ricerca anche sulla Cybersecurity.

3.3 Cybersecurity

Contesto attuale, motivazioni ed evoluzioni

La sicurezza delle comunicazioni digitali e di ciò che saranno nei prossimi anni l'Internet delle Cose e l'Intelligenza Artificiale sono tra le principali preoccupazioni dei governi mondiali. Il lavoro, l'economia, gli scambi, il tempo libero delle persone si svolgono oggi per buona parte online, senza che vi sia una reale consapevolezza a livello sociale, aziendale, politico e individuale dei pericoli connessi.

Il cyberspace è difatti la cosa più complessa che l'uomo abbia mai costruito. Esso è, da un lato, il risultato dell'unione di centinaia di migliaia di reti che rendono difficile anche solo avere una fotografia istantanea di chi vi è connesso e, dall'altro, della stratificazione di hardware, di programmi software e di protocolli sviluppati negli ultimi cinquant'anni. Questa complessità è generatrice di vulnerabilità (dovute a errori software, errate configurazioni, debolezze nei protocolli, errori nei dispositivi hardware, inserimento di dati spuri nel processo di apprendimento dell'Intelligenza Artificiale) che vengono sfruttate da cyber-criminali e da attori statuali per sottrarre dati o arrecare danni. Blocco dell'operatività di aziende, controllo surrettizio di servizi di infrastrutture critiche, furto della proprietà intellettuale o di informazioni cruciali per la sopravvivenza di un'azienda, furti di identità sono esempi delle minacce che un Paese deve affrontare. Le recenti campagne di ricatti on line (*ransomware*) e di sottrazione dati sono state gli eventi visibili di una serie di attacchi in ogni angolo del pianeta.

Gli attacchi informatici suscitano allarme nella popolazione, causano danni all'economia e mettono in pericolo la stessa incolumità dei cittadini quando colpiscono le reti di distribuzione di servizi essenziali come la sanità, l'energia, i trasporti, vale a dire le infrastrutture critiche per la società moderna. In Italia, interi settori di eccellenza, come la meccanica, la cantieristica, il Made-in-Italy, il turismo, i beni culturali, l'agroalimentare e i trasporti, potrebbero subire pesanti riduzioni del loro giro d'affari, a causa di attacchi perpetrati nel cyberspace da concorrenti commerciali, dalla criminalità organizzata, ma anche da stati sovrani. Questi attacchi possono peraltro essere dissimulati e scaglionati nel tempo, in modo da ridurre le prestazioni delle tecnostrutture attaccate nel medio e lungo periodo, con conseguenze economiche altrettanto gravi. Le corrispondenti minacce, dette Advanced Persistent Threat, rappresentano un problema fondamentale per tutte le grandi organizzazioni. Gli attacchi possono compromettere in breve tempo la credibilità di un'azienda, oppure farla operare per lungo tempo in condizioni sub-ottime, minando lo sviluppo del suo business e la capacità di vendere prodotti. Un attacco riuscito potrebbe destabilizzare il mercato azionario o obbligazionario, facendo sprofondare interi Paesi nel caos, oppure agire sui componenti hardware e software delle reti di distribuzione, bloccando, ad esempio, i rifornimenti di gas o il ciclo dei rifiuti urbani.

Non solo l'industria, ma anche la democrazia viene continuamente attaccata nel cyberspace. Le *fake news* sono l'evoluzione degli attacchi basati su *ingegneria sociale*: confezionate, personalizzate e diffuse in modo mirato attraverso il cyberspace, le false informazioni tendono a confondere i cittadini e destabilizzare i paesi. Nell'ultima relazione[7] dei Servizi di Informazione e Sicurezza al Parlamento Italiano viene infatti sottolineato come le campagne volte a influenzare l'orientamento e il sentimento dell'opinione pubblica, abbiano "dimostrato di saper sfruttare, con l'utilizzo di tecniche sofisticate e di ingenti risorse finanziarie, sia gli attributi fondanti delle democrazie liberali (dalle libertà civili agli strumenti tecnologici più avanzati), sia le divisioni politiche, economiche e sociali dei contesti di interesse, con l'obiettivo di introdurre, all'interno degli stessi, elementi di destabilizzazione e di minarne la coesione".

Molte volte i danni derivanti da attacchi informatici dipendono da un anello debole facilmente identificabile: l'essere umano. Con l'avvento dei sistemi cyber-fisici e l'evoluzione guidata dalle tecnologie IT dei sistemi di controllo e di gestione, l'uomo diventa parte integrante del cyberspace e il *fattore umano* rappresenta la più importante e impredicibile vulnerabilità di questo macrosistema. Un *click* sbagliato può infatti rendere inutile qualsiasi linea di

[7]https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2020/03/RELAZIONE-ANNUALE-2019-4.pdf

difesa tecnologica di un apparato, di una organizzazione, di un Paese. Le vittime di campagne di *phishing* mirato, le persone che usano password banali o che usano lo stesso dispositivo per giocare e per accedere alla rete aziendale, possono aprire le porte ai criminali verso i siti, le reti e le basi dati della loro organizzazione, con effetti pericolosi e imprevedibili.

Si pone quindi il problema di come difendere il cyberspace dalle minacce e dagli attacchi che, attraverso azioni informatiche di carattere malevolo, portano a compimento truffe, rubano dati sensibili e strategici per le aziende e condizionano la stabilità finanziaria, l'ordine pubblico e la vita democratica di un Paese.

La sfida cyber è molto impegnativa perché le minacce connesse alla rivoluzione digitale corrono molto più velocemente delle strategie di difesa e delle politiche pubbliche. Ciò è anche dovuto alla diffusione delle informazioni e della conoscenza (se usate in maniera impropria) attraverso la rete Internet. Per questo è particolarmente importante coinvolgere in modo sempre più intenso e integrato istituzioni, università, centri di ricerca e imprese. Un Paese che non metta la cybersecurity al centro delle proprie politiche di innovazione e trasformazione digitale pone a serio rischio la propria prosperità economica e la propria indipendenza.

Impatto sugli assi portanti della nostra società

La trasformazione digitale sta interessando tutti i settori della nostra economia e sta cambiando profondamente la società, le nostre relazioni e il modo di fare industria. Le attività più importanti si svolgono prevalentemente nel cyberspace dove cittadini, organizzazioni e cyber-criminali di ogni zona geografica operano in ambiti contigui e debolmente separati, a pochi "click" di distanza uno dall'altro. L'hardware, il software, i sistemi di interconnessione, i processi aziendali e amministrativi, i contratti, le politiche di sviluppo, le persone, le interazioni interpersonali possono essere compromesse da attacchi cyber di vario tipo. La cybersecurity è pertanto un elemento essenziale per garantire, nel tempo, un adeguato livello di sicurezza alle nostre relazioni, ai nostri affari, alle nostre democrazie. Inoltre, la messa a punto di tecniche per garantire il rispetto della privacy, oltre a preservare valori fondanti della nostra società, porterà all'aumento della fiducia collettiva nell'infrastruttura tecnologica nazionale e ne aumenterà le caratteristiche competitive.

In questa sezione, si analizza l'impatto della trasformazione digitale su alcuni tra i più importanti settori portanti della società e la rilevanza delle opportune politiche di cybersecurity.

Democrazia

Per uno stato democratico è indispensabile raggiungere un elevato livello di cybersecurity per garantire sia la sicurezza nazionale (incluse la tutela di libere elezioni e la protezione delle campagne elettorali da interferenze esterne) sia il benessere economico e la crescita del Paese. Questo obiettivo richiede un serio impegno a sviluppare strategie nazionali che allineino i bisogni di sicurezza nazionale con i diritti individuali, caratteristici delle democrazie, e con le esigenze di crescita economica, promuovendo la sicurezza sin dalla progettazione delle politiche digitali e delle normative correlate. Questo impegno dovrà essere accompagnato da iniziative di formazioni sul territorio che, coinvolgendo università e aziende, offrano ai cittadini occasioni di consapevolezza delle problematiche di cybersecurity e di formazione e crescita.

Finanza

Il settore finanziario subisce da decenni attacchi sempre più sofisticati, caratterizzati da vettori di attacco distribuiti e coordinati. L'analisi degli attacchi permette di individuare tre minacce fondamentali: (i) compromissione temporanea delle funzionalità dei servizi bancari e assicurativi, (ii) furti e truffe organizzate su larga scala di dati bancari e finanziari, (iii) violazione dell'integrità dei dati presenti all'interno del sistema bancario anche attraverso l'apertura di falle permanenti che permettano l'esfiltrazione non autorizzata di informazioni. Le minacce cyber ai servizi bancari possono dare origine a un rischio sistemico per la stabilità finanziaria. Attacchi coordinati possono portare a una compromissione della capacità di iniettare capitali e liquidità nel sistema delle imprese. L'approccio puramente passivo e difensivo potrebbe essere a lungo termine insostenibile senza un'azione proattiva di *cyber-intelligence* che

individui i vettori d'attacco più critici, che tendono a variare nel tempo. Un fattore di rischio per le assicurazioni nasce invece dalla difficoltà di garantire la sicurezza dei dispositivi IoT che sono sempre di più integrati nei nuovi servizi assicurativi. In questi servizi, l'ammontare dei premi viene legato al rischio stimato attraverso dati ambientali e la sostenibilità dei contratti dipende dall'integrità dei dati forniti dai sensori.

Infrastrutture

La resilienza del sistema Paese si fonda anche sulla disponibilità di un insieme di infrastrutture che, a causa del ruolo che in esse riveste l'IT, fanno a pieno titolo parte della superficie d'attacco cyber per la quale sono necessarie specifiche azioni di protezione. Il primo punto di attenzione è quello relativo alle infrastrutture di rete, ai data center, e alle infrastrutture di cloud computing, che sono elementi fondamentali della trasformazione digitale del Paese e fattori critici per il funzionamento di servizi essenziali. Un altro segmento importante è rappresentato dalle infrastrutture energetiche, e cioè la rete nazionale dei gasdotti e la rete elettrica di trasmissione nazionale. Le problematiche di cybersecurity in questo ambito sono prioritarie, viste le possibili conseguenze potenzialmente catastrofiche che gli attacchi informatici a queste infrastrutture possono determinare. In tale ambito, la ricerca dovrà anche misurarsi con l'evoluzione delle reti energetiche che nei prossimi anni includeranno il paradigma delle smart-grid, il cui modello decentralizzato apre nuovi scenari di rischio cyber. Non sono da trascurare anche le infrastrutture per la gestione delle risorse idriche e delle acque reflue, le cui componenti IT (sensori, attuatori, sistemi SCADA) sono spesso presi di mira dai criminali informatici.

Trasporti

La cybersecurity nell'ambito trasporti richiede di considerare allo stesso tempo i veicoli, i servizi e le infrastrutture cosiddette "smart". Per i veicoli e i servizi, la sempre maggior diffusione di dispositivi IoT, che permette sia di migliorare il comfort dei passeggeri sia di offrire servizi innovativi a livello di guida assistita o semi-autonoma, introduce nuove sfide per la cybersecurity relative all'aumento smisurato della superficie di attacco e al trattamento sicuro della grande mole di dati generati, nonché ai potenziali effetti sulla componente umana coinvolta. Gli attacchi ai sistemi di trasporto, che hanno caratteristiche simili ai sistemi di controllo industriali, sono diversi dai tradizionali attacchi alle infrastrutture ICT. Storicamente i sistemi di trasporto usano protocolli "legacy" che nel tempo sono diventati vulnerabili ad attacchi mirati. Questi sistemi però possono funzionare per mesi o anni senza interruzione, e risulta difficile aggiornare o persino riavviare gli apparati che li controllano per introdurre nuove versioni dei controlli di sicurezza. Relativamente alle infrastrutture, è necessario definire nuovi standard in grado, al contempo, di integrare quelli esistenti e di affrontare efficacemente le problematiche di safety e di cybersecurity introdotte dal fatto che veicoli e infrastrutture sono sempre più interconnessi e accessibili anche dai potenziali attaccanti.

Industria

La trasformazione digitale sta cambiando profondamente il modo di fare industria. La nuova industria, definita 4.0, perderà completamente il concetto di perimetro fisico: l'IoT, l'intelligenza artificiale, i dispositivi mobili, il cloud stanno eliminando completamente il concetto di perimetro aziendale, spostando dati e servizi al di fuori di esso. A livello aziendale esistono numerosi rischi legati alla cybersecurity ed è importante che vengano definiti meccanismi per garantire livelli di sicurezza adeguati sia per i dispositivi hardware e software che entrano nel perimetro aziendale sia per l'intera catena di approvvigionamento (supply chain), tenendo presente che mai come per la cybersecurity la robustezza di una catena è quella del suo anello più debole.

Sanità

Il sanitario è uno dei settori maggiormente esposti ad attacchi informatici che possono compromettere non solo la privacy degli utenti, ma anche l'efficienza dei processi e la salute dei cittadini. Mentre è sicuramente di primaria importanza proteggere da attività indebite tutti i dati sanitari in modo uniforme su tutto il territorio nazionale, va rimarcato che dispositivi medici digitali vulnerabili possono mettere a rischio pazienti ed operatori ed è quindi altrettanto necessario che sia la produzione sia l'utilizzo di tali dispositivi vengano supportati dall'introduzione di adeguate misure di protezione e di strategie di mitigazione dei rischi ritenuti elevati.

Obiettivi di ricerca per la cybersecurity (2021-2027)

Il ruolo della ricerca scientifica è fondamentalmente per affrontare le grandi sfide insite negli ambiti appena visti. In molti casi, oltre ai risultati teorici a lungo termine, è necessaria la realizzazione di sistemi prototipali propedeutici alla fase di industrializzazione delle soluzioni. Questi obiettivi potranno essere raggiunti stimolando la nascita di spin-off o start-up, con l'aumento di pubblicazioni e di brevetti e il trasferimento dei risultati dalle pubblicazioni alle applicazioni.

La realizzazione degli obiettivi, data la loro diversità e la varietà delle competenze necessarie, richiede una forte sinergia tra il mondo della ricerca scientifica e quello della ricerca industriale. In particolare, le aziende avranno un ruolo fondamentale nelle fasi di prototipazione e industrializzazione. Il rapporto tra ricerca e industria dovrà essere di tipo *circolare*, nel senso che (i) i problemi affrontati dovranno essere definiti in modo condiviso; (ii) gli approcci innovativi dovranno essere definiti sulla base di scenari e requisiti individuati in modo collaborativo; (iii) le soluzioni sviluppate dovranno essere modificate e raffinate sulla base delle esperienze industriali *sul campo*. Tutto ciò permetterà di realizzare un trasferimento tecnologico tempestivo ed efficace. Di seguito vengono delineati alcuni degli obiettivi che il *Sistema Ricerca Italiano* deve perseguire per mirare a garantire sicurezza sociale ed economica anche garantendo cybersecurity.

Proteggere Dati e Servizi in Rete

Le applicazioni e i servizi in rete stanno rapidamente diventando il canale preferito dagli utenti per l'accesso ai servizi digitali erogati dalle pubbliche amministrazioni, dalle aziende e dalle banche. Si pensi, ad esempio, ai servizi erogati dai portali dell'INPS e dall'Agenzia delle Entrate, ai servizi di biglietteria digitale e all'home banking. Tali applicazioni consentono di effettuare operazioni che presuppongono elevati standard di sicurezza, sia per la sensibilità dei dati trattati sia per l'impatto economico o reputazionale che un abuso del servizio da parte di malintenzionati comporterebbe. Spesso servizi avanzati sono erogati combinando sistemi diversi che interagiscono, dando vita a veri e propri "ecosistemi". Le organizzazioni devono quindi essere messe in grado di creare servizi innovativi basati sui dati, rispettando al contempo la legislazione sulla loro protezione e sulla privacy. È pertanto importante disporre di metodologie, strumenti e informazioni per valutare, analizzare e misurare il livello di sicurezza (e privacy) delle singole componenti, dei sistemi ottenuti tramite la loro interazione e degli ecosistemi derivanti dalla composizione di altri sistemi, perseguendo i seguenti obiettivi di ricerca:

- **Certificazione di applicazioni con dati sensibili**: È necessario sottoporre le applicazioni alle opportune certificazioni sia prima del loro utilizzo, sia durante il loro funzionamento, tenendo conto delle variabilità dovute all'interazione con le componenti individuate al momento dell'esecuzione.
- **Analisi automatica di applicazioni**: Occorre sviluppare metodologie automatiche di analisi di sicurezza, configurazione, gestione e test per applicazioni complesse, tenendo conto della varietà degli schemi di composizione.
- **Analisi di sistemi interoperanti**: È necessario sviluppare metodologie e strumenti per l'attestazione di integrità a livello di infrastruttura e di componenti e di protezione dei dati acquisiti e gestiti.

Individuare Malware

I malware rappresentano una delle minacce principali nell'ambito della cybersecurity essendo sia veicoli per accedere a un sistema remoto, per controllarlo e comprometterlo, sia strumenti per la sottrazione o distruzione di informazioni presenti in sistemi informatici. Gli obiettivi principali da perseguire in questo ambito possono essere così riassunti:

- **Raccolta e validazione di insiemi di dati** rappresentativi di comportamenti normali o anormali a uso dei modelli di classificazione basati su apprendimento automatico.
- **Creazione di una banca dati nazionale** di codice malevolo, costruita a partire da un'infrastruttura che raccolga e permetta di coordinare le risposte in caso di attacco malware e che si integri con le banche dati almeno dei paesi europei.

- **Sviluppo di un insieme di strumenti e metodologie** per la sorveglianza automatica del cyberspace e l'individuazione preventiva di campagne di malware attraverso il monitoraggio e il raggruppamento di tali campagne in base ai canali di comunicazione utilizzati, al codice utilizzato o ai server remoti che li controllano e che, appena individuati, potrebbero essere inseriti in *blacklist*.

Combattere il Cybercrime

Gli incidenti legati alla sicurezza informatica sono di natura eterogenea e vanno dal furto di identità al cyber-spionaggio, dalle truffe finanziarie ai *ransomware* al *cyberterrorism*. Questo fenomeno è la conseguenza di un'evoluzione paradigmatica del cyber-crime, che oggi agisce anche secondo un modello di *crime-as-a-service* in cui strumenti di attacco estremamente potenti e complessi diventano accessibili a prezzi contenuti e possono essere utilizzati senza richiedere competenze tecniche approfondite. Attacchi recenti hanno mostrato come i cyber-criminali siano in grado di infiltrarsi in organizzazioni complesse, prendere il completo controllo di sistemi di larga scala, e persistere per anni in tali sistemi nascondendo efficacemente la loro presenza. Questo tipo di attacchi rappresenta un problema fondamentale per tutte le grandi organizzazioni e aziende. I principali obiettivi di ricerca da perseguire sono, pertanto, i seguenti:

- **Threat intelligence avanzata:** Sviluppo di piattaforme di *Threat intelligence* che permettano la costruzione di una base di conoscenza condivisa a livello mondiale relativa a gruppi cyber-criminali, minacce e attacchi.
- **Identificazione di vulnerabilità in ambienti complessi**: Sviluppo di strumenti e metodi per il monitoraggio continuo e l'analisi dei sistemi per l'identificazione di possibili vulnerabilità e di possibili strategie di attacco da cui difendersi.
- **Automazione delle indagini forensi:** Sviluppo di strumenti finalizzati all'analisi automatizzata dei sistemi oggetto di attacco, al fine di estrarre e correlare in modo automatizzato informazioni legate alle attività dell'attaccante.

Difendere la Democrazia e combattere le Fake News

Il processo di diffusione delle informazioni false passa per una serie di meccanismi cognitivi che porta ad acquisire le informazioni coerenti con la propria visione del mondo e a ignorare le tesi a contrasto. Questo rende feconda la diffusione di informazioni false a fini economici e sociali. Il problema è serio e delicato e la scienza in generale e l'informatica in particolare debbono svolgere un ruolo fondamentale in questa sfida. I principali obiettivi da perseguire sono i seguenti:

- **Approccio multidisciplinare** per mettere in atto una serie di iniziative e sinergie volte a garantire una migliore comprensione del problema e a predisporre risposte efficaci.
- **Monitoraggio dei social media** per individuare e seguire la dinamica degli algoritmi di confinamento informativo che danno luogo alle cosiddette *echo-chamber* nelle quali si tende a rinforzare i punti di vista comuni e ad attenuare, se non a eliminare, quelli dissonanti.
- ***Early Warning*** sui messaggi che possano essere veicolo di informazioni false, fuorvianti o strumentali, usando classificatori che si basano su caratteristiche sintattiche, semantiche, ma anche sulla la rete dei flussi di informazione.
- **Fattore Umano** da considerare per alleviare le vulnerabilità dei sistemi mettendo in opera tecniche di previsione del comportamento e di analisi del rischio conciliandole con il rispetto della privacy e dei diritti individuali dei cittadini.

Integrare Intelligenza Artificiale e Cybersecurity

Le capacità dei modelli di apprendimento automatico stanno crescendo a un ritmo senza precedenti e l'Intelligenza artificiale (IA) basata su di essi sta attirando tantissima attenzione. Difatti, l'IA può essere uno strumento importante

per la messa a punto di strategie di difesa, per rilevare comportamenti anomali e prevedere possibili attacchi. Ma, dal punto di vista della cybersecurity, essa va vista anche come una tecnologia da proteggere e come tecnologia da cui proteggersi. In particolare, i dati con cui si addestrano i modelli dell'IA possono essere inquinati con scopi malevoli per eludere tentativi di difesa e, opportunamente modificati, per indurre i sistemi a trarre conclusioni diverse da quelle dovute. A titolo di esempio, un avversario può acquisire informazioni riservate, o classificate, dai dati usati per l'addestramento di un sistema o può influenzarne il processo di apprendimento "avvelenando" i dati dell'addestramento. In certi casi, l'inquinamento può avvenire anche dopo la messa in opera dei modelli, sfruttandone la plasticità residua, peraltro indispensabile per gestire la non stazionarietà dei fenomeni che vengono considerati. È pertanto fondamentale capire le potenziali minacce alla sicurezza derivanti da usi malevoli dell'IA per prevedere, prevenire e mitigare le minacce, ed è pertanto necessario:

- **Rilevare data o code injection** per combattere tentativi di clonazione di modelli e l'inserimento di dati falsi o modificati nella fase di addestramento o di test dei sistemi IA;
- **Definire algoritmi di learning più robusti,** che siano resilienti ad attacchi e garantiscano il mantenimento di funzionalità attese e che siano possibilmente testati tramite tecniche di "red teaming" proprie della cybersecurity.
- **Sviluppare tecniche per preservare l'integrità dei dati in addestramento e in produzione**, garantendo la fiducia nelle procedure di sintesi dei modelli partendo dai dati.
- **Preservare la privacy,** sviluppando approcci all'addestramento che non rivelino dati sensibili e individuando metodologie per misurare la vulnerabilità e la resilienza dei sistemi IA ai cosiddetti *adversarial attack*.
- **Sviluppare strumenti di protezione basati sull'IA** per anomaly detection, fake indentity e per l'individuazione di preferenze di politiche di privacy.

Garantire la Privacy

L'utilizzo dei dati personali sia per i servizi digitali sia per la ricerca è inevitabile, ma esso porta con sé nuove sfide connesse alla privacy dei cittadini, specialmente quando i dati sono memorizzati su server nel cloud. Se questo problema non viene affrontato adeguatamente le opportunità derivanti dall'uso di grandi quantità di dati in medicina, in economia e nella ricerca scientifica in generale diventeranno anche minacce per gli individui e la società e un ostacolo per lo sviluppo di *open data* che possono contenere dati personali. Il GDPR ha definito gli standard elevati dell'UE per quanto riguarda il diritto alla privacy, la protezione dei dati personali e la tutela dei diritti fondamentali nell'era digitale. Per conciliare tutto questo con la necessità di elaborare grosse quantità di dati è necessario sviluppare ricerche su:

- **Crittografia omomorfa** che permette di elaborare direttamente dati cifrati, quindi non leggibili dai proprietari dei server che li ospitano.
- **Protezione di infrastrutture di dati federate** in spazi di dati internazionali quale ad esempio lo spazio europeo dei dati sanitari, per prevenire sia il furto di dati medici sia le violazioni della privacy dei pazienti attraverso l'analisi delle interrogazioni.
- **Anonimizzazione dei dati** per garantire l'impossibilità di re-identificazione dell'utente e permettere condivisione pubblica di informazioni su gruppi di dati evidenziando pattern dei gruppi ma nascondendo informazioni sugli individui.
- **Secure multi-party computation** per utilizzare tecniche che prevedono il coinvolgimento nell'elaborazione di più componenti senza che nessuna di esse abbia una visione complessiva degli input privati.
- **User-centric privacy** per definire modelli e politiche di controllo dell'accesso in grado di esprimere requisiti di privacy in conformità a normative (tipo GDPR) e di garantire che il controllo sui dati venga mantenuto dai rispettivi titolari.

Prepararsi agli attacchi dei Computer Quantistici

L'avvento di computer quantistici potrebbe mettere in crisi i sistemi a chiave pubblica di largo utilizzo ed è quindi importante studiare algoritmi crittografici post-quantum che siano robusti rispetto a tecnologie che, già disponibili oggi, ma non utilizzabili in pratica per ragioni di scala/capacità, saranno disponibili con una capacità (numero di qubit) adeguata tra pochi anni. Molte aziende e governi non possono permettere che in un futuro non troppo remoto le loro comunicazioni e i loro dati vengano decifrati o le firme digitali vengano falsificate. Tuttavia, se da un lato i calcolatori quantistici aprono la strada a nuovi possibili attacchi ai sistemi crittografici, le tecnologie quantistiche permettono anche di sviluppare sistemi di comunicazione intrinsecamente sicuri, che possono essere utilizzati per la distribuzione di chiavi crittografiche. Pertanto, prima che i computer quantistici diventino accessibili su larga scala, è importante:

- **Progettare nuovi sistemi di crittografia** il cui livello di sicurezza sia quantificabile, con precisione, rispetto alla crittoanalisi, considerando dispositivi sia quantistici sia classici;
- **Studiare l'usabilità di sistemi crittografici e dei metodi di generazione e distribuzione delle chiavi basati su tecnologia quantistica** per i dispositivi di calcolo di uso generale;
- **Garantire interoperabilità** tra sistemi di crittografia quantistica e i protocolli e le reti di comunicazione classiche.

Difendere l'Hardware

L'hardware gioca un ruolo chiave nella sicurezza di qualsiasi sistema informatico; da un lato, infatti, un hardware vulnerabile può compromettere tutte le soluzioni di sicurezza implementate tramite i programmi che esegue e, dall'altro, un hardware "fidato", all'interno di un sistema può fornire una "chain of trust" basata sul silicio e a esso "ancorata", in grado di rendere più affidabili e sicuri i dispositivi e le reti. L'esigenza di "protezione" delle infrastrutture hardware, ribadita peraltro anche da recenti normative sia comunitarie sia nazionali, richiede oggi significativi investimenti in termini di ricerca, specialmente in un Paese come il nostro che, a causa di specifiche scelte industriali e politiche, si trova da anni a dipendere completamente da fornitori stranieri per l'approvvigionamento di dispositivi hardware di ultima generazione. Per questo è necessario supportare ricerche che puntino a:

- **Individuare tecnologie hardware da sviluppare a livello nazionale** per ridurre la marginalità tecnologica nel settore e controllare totalmente l'intera filiera, che va dalla progettazione al processo di produzione, al collaudo, alla certificazione, alla installazione, alla manutenzione, agli aggiornamenti e alla dismissione.
- **Progettare architetture nazionali tolleranti le vulnerabilità**, in grado di garantire livelli di sicurezza predefiniti, anche in sistemi potenzialmente vulnerabili, che, sviluppati secondo i paradigmi della *Security by Design*, siano in grado di fornire livelli di sicurezza variabili e adattabili alle diverse criticità dei sistemi.

Strumenti necessari per garantire cybersecurity

Concludendo questa parte introduttiva, si ritiene utile sottolineare che la spesa per lo sviluppo di metodologie e tecnologie di cybersecurity rappresenta un investimento che è funzionale ad aumentare la resilienza e la sostenibilità dei servizi e delle infrastrutture del nostro Paese ed a sostenere una strategia di sviluppo di breve e medio termine.

Nel resto di questo documento vengono dettagliati i principali strumenti necessari per raggiungere gli obiettivi appena delineati; in particolare, vengono prese in considerazione diverse articolazioni:

1. *Intelligence and Incident response*: Considera gli strumenti necessari per individuare preventivamente possibili vulnerabilità e vettori di attacco e, quindi, per risolvere tali vulnerabilità e rispondere tempestivamente agli attacchi cyber.
2. *Sicurezza dei sistemi cyber-fisici e delle infrastrutture di rete*: Si occupa di proteggere i servizi erogati da sistemi con forte interazione con l'uomo, che tradizionalmente erano meccanici ma che sono via via sempre più interconnessi e pervasivi; si tratta di sistemi di supporto per infrastrutture critiche, trasporti, industria, applicazioni mediche e biomedicali, tecnologie assistive.

3. *Tecniche e metodologie per la protezione delle risorse*: Analizza l'uso della crittografia per proteggere le informazioni e mitigare i rischi connessi all'avvento dei quantum computer, le nuove tecniche per la regolamentazione dell'accesso, le tecniche di protezione hardware e le relazioni tra Intelligenza Artificiale e cybersecurity sia come strumenti di difesa sia come tecnologie da difendere.
4. *Sicurezza dei servizi al cittadino e alle imprese*: Si occupa dell'uso dell'enorme quantità di dati prodotti dai dispositivi digitali, e di come questi possano essere trattati nell'interesse dei cittadini e delle imprese garantendo qualità dei servizi, affidabilità delle informazioni e privacy.
5. *Ecosistema della Cybersecurity*: Analizza il sistema complesso della cybersecurity partendo da una visione orientata ai processi di gestione, certificazione, assessment, standardizzazione e compliance per proporre linee di ricerca per un framework di governo della cybersecurity basato sulla gestione del rischio di processi, servizi e prodotti.
6. *Infrastrutture di Ricerca per la Cybersecurity*: Propone la creazione di centri di ricerca nazionali, territoriali o settoriali, nonché lo sviluppo di infrastrutture per il monitoraggio di attacchi informatici e di infrastrutture di libro mastro distribuito che risultino funzionali allo sviluppo di servizi sicuri forieri di significativi vantaggi economici e di competitività.

Articolazione 1. Intelligence and incident response

La possibilità di individuare per tempo possibili minacce e di rispondere tempestivamente agli attacchi è una tematica di rilevante interesse per il sistema nazionale, in funzione del crescente incremento del rischio cyber rispetto ad asset e operatori essenziali dello Stato. L'avanzamento della conoscenza scientifica nel campo delle metodologie e delle tecnologie orientate alla prevenzione, identificazione, gestione, contenimento, analisi di attacchi cyber appare pertanto tra le principali priorità, anche al fine di consolidare strutturalmente le capacità del Paese nella difesa del dominio cyber. Vi sono diverse linee di intervento verso le quali appare strategico orientare la ricerca nazionale. Tra queste certamente lo sviluppo di metodologie e tecnologie di *intelligence* per l'identificazione e il contrasto delle attività di *cybercrime e cyberterrorism*, attraverso uno sforzo multidisciplinare che tenga anche conto delle componenti socioeconomiche e politiche delle reti criminali organizzate. È cruciale anche dare impulso all'*offensive security*, non riferendosi necessariamente a scenari di *cyberwar*, ma al fatto che la protezione del proprio dominio cyber può realizzarsi efficacemente solo se si è in grado di testarne la robustezza con le armi di un attaccante. Un capitolo specifico è quello relativo ad analisi, classificazione, e rilevamento dei *malware*, che rappresentano una delle minacce principali alla sicurezza dei sistemi di *Information Technology* (IT) e *Operation Technology* (OT). L'analisi dei malware, così come le strategie di *attack detection,* rientrano nel dominio più vasto dell'*incident response*, intesa come la capacità delle organizzazioni di identificare, classificare, prioritizzare, analizzare prontamente attacchi informatici, e attuare strategie di contenimento e remediation, oltre che di *digital forensics*, per un'analisi post-mortem dell'incidente e l'estrazione di evidenze e prove.

In questo settore, la ricerca deve concorrere all'innalzamento delle conoscenze scientifiche e tecnologiche utili al consolidamento di una visione della cybersecurity che pone l'accento sulle capacità delle organizzazioni, dalla più semplice alla più complessa, di contrastare e prevenire gli attacchi informatici attraverso un approccio attivo, eventualmente attuato *sul campo,* che si fonda principalmente sulla conoscenza delle strategie utilizzate dagli attaccanti, fino all'adozione della loro stessa *forma mentis* a scopo di difesa e prevenzione. Ciò si può declinare verso molteplici direzioni, che potranno ricondurre a diversi obiettivi di ricerca:

A. **Metodologie e tecnologie per l'Intelligence**
B. **Offensive Security per finalità di difesa**
C. **Processi di incident response**
D. **Miglioramento delle capacità di difesa rispetto al malware**

Obiettivi

A. Metodologie e tecnologie per l'Intelligence

L'obiettivo di ricerca va inteso come miglioramento della capacità di attuare la tutela della sicurezza di un sistema (possiamo riferirci al sistema Paese o a sue macrocomponenti) e la prevenzione di eventi che possano minarne la stabilità. Nel dominio cyber non è solo il *cybercrime* a dover essere oggetto di attenzione da parte delle attività di intelligence, ma anche il *cyberterrorism,* per i connotati specificatamente informatici che lo caratterizzano e le relative sfide che devono essere affrontate attraverso metodologie informatiche. Obiettivi di ricerca specifici riguardano pertanto la capacità di raccogliere, mantenere, analizzare informazioni e dati provenienti da ogni possibile fonte al fine di contrastare e prevenire tali minacce. A tal fine, sono identificabili i seguenti obiettivi prioritari:

- *Metodologie e strumenti a supporto delle attività di OSINT* (Open Source INTelligence). Ciò richiede, in linea generale, lo sviluppo di una migliorata capacità di estrarre conoscenza da fonti estremamente eterogenee, fronteggiando la straordinaria dimensione del dominio soggetto all'analisi sia dal punto di vista semantico sia da quello dell'efficienza computazionale. Ciò si traduce nell'abilità di effettuare una sintesi di svariati approcci, che vanno dal *Natural Language Processing,* al *Text/Data Mining*, per citare alcuni esempi di tematiche afferenti all'ambito dell'Intelligenza Artificiale (che in questo contesto, anche nelle declinazioni orientate al *ragionamento deduttivo* e agli approcci *rule-based*, può trovare ampia applicazione), ma riguardano anche il dominio delle *Complex Network*, con specifica attenzione verso la *social network analysis*, includendo gli aspetti di acquisizione delle informazioni da fonti social e quelli specifici dell'ambito dei *big data* per l'analisi efficiente di grandi moli di dati.
- *Fornire valore aggiunto alla threat intelligence* attraverso un maggiore supporto scientifico agli approcci operativi e un maggiore grado di automazione, incrementando anche l'efficacia applicativa dell'azione. La threat intelligence è vista come insieme di metodologie atte a identificare minacce cyber emergenti attraverso la raccolta delle informazioni che ne delimitano i contorni e che costituiscono la base dei processi decisionali di risposta. In tale ambito, obiettivi specifici sono quelli della definizione di processi il più possibile automatizzati per l'acquisizione di informazioni da sorgenti protette, tipicamente appartenenti al dominio del *dark web*. Altro aspetto di rilievo che conduce alla definizione di ulteriori obiettivi specifici riguarda il monitoraggio continuo e l'identificazione precoce di indicatori che possano supportare il rilevamento delle compromissioni. In questo contesto, assume un ruolo fondamentale lo studio di adeguati modelli e protocolli di *information sharing*, non solo in termini di organizzazione dei flussi informativi e dei ruoli dei diversi attori in gioco, ma anche in relazione all'organizzazione strutturale e semantica delle informazioni condivise e al loro trattamento, il tutto finalizzato allo scopo di alimentare e supportare efficacemente primariamente le piattaforme di incident response (SIEM) e dei *Security Operation Center* (SOC), ma anche i sistemi e le strategie di *antifrode* e di *antiriciclaggio*, detti anche *anti money laundering (AML).*
- *Migliorare la capacità di comprendere i fenomeni del cybercrime e del cyberterrorism*. L'obiettivo riguarda l'adozione e la specializzazione delle metodologie di cyber-intelligence al fine di incrementare la capacità di indagine e di prevenzione delle azioni avverse. È necessario, per entrambi i fenomeni, comprenderne organizzazione, dislocazione e dinamiche, includendo fattori sociali, politici, economici e giuridici. Partendo dagli aspetti modellistici ispirati alla *teoria dei giochi*, fino a punti più concreti volti a studiare ed identificare i connotati specifici dei due domini e dei suoi attori, e gli impatti che essi sono in grado di determinare sui diversi segmenti della società, è necessario prevedere attività di ricerca fortemente interdisciplinari strategiche ai fini della lotta al crimine informatico e al cyber-terrorismo
- *Consolidare gli approcci cybersecurity-based per il contrasto al cyberterrorism*. L'utilizzo di Internet, incluso il dark web, da parte delle reti terroristiche internazionali, pone sfide di ricerca per le quali le competenze in cybersecurity possono svolgere un ruolo determinante. Similmente a quanto accade per il cybercrime, diverse aree disciplinari possono essere coinvolte in attività di ricerca secondo un approccio intrinsecamente interdisciplinare nel quale, però, gli specifici connotati cyber del fenomeno, rendono imprescindibile l'adozione di un punto di vista *cybesecurity-based*. Gli approcci afferenti al dominio della *cyber-intelligence* visti precedentemente, opportunamente declinati nel dominio del terrorismo, trovano piena applicazione,

attraverso l'identificazione di comunicazioni, reti e organizzazioni terroristiche, ma anche di singoli individui che possono rappresentare una possibile minaccia, si pensi per esempio al fenomeno della radicalizzazione che può avere dei precisi pattern. In questo dominio vi dovrà essere una specifica attenzione nei riguardi delle tecniche di crypto-analysis e stego-analysis, visto il diffuso ricorso all'information hiding (anche con mezzi di comunicazione non convenzionali -- come ad esempio il *gaming* online) da parte delle reti terroristiche.

- *Definire modelli e metodologie per il supporto al contrasto del crimine*. Anche al di fuori del dominio del cybercrime, il mondo del crimine fa largo uso di strumenti IT e di comunicazione, che sono certamente un mezzo di straordinaria importanza investigativa. Tuttavia, le attività di intercettazione, anche di comunicazioni cifrate o che sfruttano metodi di information hiding, sia per le sfide di natura tecnologica che di volta in volta si possono presentare, sia per la necessità di garantire che il processo avvenga con elevate garanzie di confidenzialità, disponibilità, integrità, e ed evidenza giuridica e processuale, necessitano di un supporto scientifico atto a identificare modelli, protocolli e metodologie specifiche. Si pensi al problema della garanzia di conformità di contenuti intercettati nel caso di riversamento con modifica di formato. Anche l'uso del captatore informatico presenta diversi aspetti critici aggravati dal fatto che l'azione è svolta attraverso software potenzialmente sviluppato e gestito da terze parti.

B. Offensive Security per finalità di difesa

L'*offensive security* include tutte quelle competenze, metodologie e tecnologie che permettono di approcciare la verifica della robustezza dei sistemi informatici attraverso le stesse armi, e lo stesso *pensiero laterale*, che adottano gli attaccanti informatici.

Gli obiettivi di ricerca specifici individuati come prioritari nell'ambito dell'*offensive security* sono*:*

- *Penetration testing*. Messa a punto di nuovi approcci e nuove metodologie, anche basate su tecniche di Intelligenza Artificiale, per avanzare lo stato dell'arte nel dominio del *penetration testing* e del *vulnerability assessmen*t.
- *Assessment di specifici domini.* Vista l'evoluzione continua della tecnologia, appare sempre attuale e cogente sviluppare modelli e metodologie specifiche di penetration test e vulnerability assessment in domini verticali, preferibilmente integrati con metodologie standardizzate di analisi dei rischi. A titolo esemplificativo, gli scenari di dematerializzazione e digitalizzazione abilitati dal regolamento europeo eIADAS e dalla direttiva PSD2, possono rappresentare un dominio applicativo nel quale è possibile identificare specifici obiettivi di ricerca in tema di offensive security, che avrebbero un impatto significativo nel processo di sviluppo dei servizi digitali in UE.
- *Miglioramento della capacità di valutazione delle metodologie.* Il tema della *valutazione* (ed eventuale *certificazione*) delle metodologie di offensive security appare particolarmente significativo, anche perché non ancora sufficientemente esplorato. Anche in questo caso non dovranno essere trascurati gli aspetti interdisciplinari del contesto in esame, nel quale le questioni di carattere etico-legale rivestono un ruolo di rilievo, per diverse implicazioni di ricerca, anche legate alla definizione di nuovi modelli di *responsible disclosure*.

C. Processi di incident response

Area di interesse contigua è certamente quella dell'*incident response*. Si può affermare che molte delle competenze menzionate prima trovano piena collocazione in un contesto organizzativo in cui si vogliano attivare dei team di risposta agli incidenti come elemento centrale di un sistema articolato nel quale convergono diversi aspetti relativi alla gestione operativa della cybersecurity in una organizzazione complessa (il riferimento principale è certamente quello dei *SOC - Security Operation Center* e degli *CSIRT - Computer Security Incident Response Team*).

In quest'ambito, diversi sono gli obiettivi di ricerca che si possono individuare, in relazione alle diverse fasi che costituiscono il processo di incident response, anche delimitando il campo di azione, e cioè immaginando attività di incident response progettate per specifici ambiti "verticali" quali sanità, energia, trasporti, settore finanziario, etc.

- *Modellazione dei processi di incident response, standard e best practice.* Tali obiettivi riguardano gli aspetti di modellazione del processo di gestione, e quindi gli *standard*, i *framework*, le *metodologie* e le *best practice*. Ancorati a questi, vi sono gli obiettivi di ricerca direttamente legati all'operatività dell'incident response, a partire dalla fase di *preparation*, relativamente all'aspetto dei *processi* e delle *procedure* e di altre attività rilevanti quali l'*asset management*, che possono trovare stretta convergenza con ambiti di ricerca della modellazione dei processi e dei *workflkow* (incluso il *workflow mining*) e dei *sistemi informativi*.
- *Incremento dell'efficacia delle fasi dell'incident response.* Tale obiettivo riguarda strettamente le attività di incident response che si originano a fronte del rilevamento dell'evento anomalo, e cioè *detection*, *analysis*, *triage*, *correlation*, *assessment*, *coordination* e *containment, digital forensics*. Anche in questo caso, pur essendo questo un ambito considerevolmente presidiato soprattutto dall'industria, come dimostrato dalla disponibilità di prodotti commerciali, appare ancora limitata l'adozione di approcci basati su una visione scientifica del problema, con l'obiettivo di rendere maggiormente automatizzabili le attività di incident response, attualmente basate sul ragionamento umano. Ciò si dovrà tradurre in un avanzamento dello stato dell'arte sia a livello metodologico sia a livello tecnologico con piattaforme dedicate quali *SIEM (Security Incident Event Management)*, e *SOAR (Security Orchestration Automation and Response*), in relazione alla loro evoluzione verso l'uso di tecniche di apprendimento computazionale.

D. Miglioramento delle capacità di difesa rispetto al malware

Nell'ambito dell'incident response, il malware ha senza dubbio un posto di rilievo. La ricerca negli ultimi anni si è concentrata quasi esclusivamente nella definizione di strumenti e metodi efficaci per il riconoscimento e la classificazione di malware. La crescita esponenziale dei volumi di malware circolanti nella rete, il conseguente incremento delle campagne di malware e gli effetti sempre più devastanti che queste sono in grado di produrre, fanno crescere l'esigenza di strumenti automatici che rendano più efficaci i meccanismi di difesa e riducano considerevolmente i tempi di risposta all'incidente, la sua gestione e il ripristino dell'area oggetto dell'attacco. Gli obiettivi di ricerca che si ritengono prioritari sono:

- *Migliorare e automatizzare le attività di malware analysis.* Da una parte, è necessario realizzare efficaci metodologie per il *malware triaging,* automatizzando le fasi preliminari dell'analisi del malware. Dall'altra, è fondamentale procedere verso l'automatizzazione della *attribuzione della paternità di un malware*. I malware vengono oggi scritti da gruppi di specialisti che operano nello spionaggio industriale, nel terrorismo, nel crimine informatico o al servizio di governi nazionali. Gli autori lasciano quasi sempre, nelle loro creazioni, tracce utilizzabili per identificarli. Lo sviluppo di metodi che siano in grado di identificare gli autori o alcune loro caratteristiche, per esempio la loro provenienza geografica, sono utili in numerosi scenari, nei quali risulti dirimente definire la provenienza del malware, oltre che essere necessario a supportare aspetti investigativi successivi all'attacco. Altra fondamentale sfida è *la caratterizzazione del payload*, questa attività è oggi non deterministica e affidata per lo più all'esperienza dell'analista o alla base di conoscenza della sandbox utilizzata. È necessario pertanto sviluppare metodologie e strumenti affidabili a supporto di questa attività.
- *Anticipare le tendenze dei nuovi malware*. I malware in circolazione sono spesso generati a partire da malware esistenti e molte delle tecniche impiegate dai codici malevoli sono evoluzioni di quelle esistenti. Basandosi su questo principio, la nostra capacità di difesa sarebbe rafforzata se potesse usufruire di sistemi in grado di prevedere le possibili evoluzioni dei malware esistenti, in termini di payload, tecniche di evasione, metodi di propagazione.
- *Sviluppare strumenti che siano in grado di fronteggiare attacchi di tipo avversariale*. L'adversarial machine learning è una tecnica che, sebbene ancora ai primordi nell'ambito della produzione di malware, può generare oggetti malevoli che confondono i classificatori tradizionali. Per questo è importante sviluppare tecniche e metodi in grado di riconoscere i malware generati da reti generative avversariali.
- *Costruire dataset rappresentativi del comportamento dei malware per la validazione di nuovi strumenti di identificazione e classificazione del malware.* La ricerca nel malware deve necessariamente utilizzare dei dataset per validare le tecniche e i metodi ideati. Questi dataset, per poter essere utilizzati diffusamente dai ricercatori

devono essere: rappresentativi della popolazione dei malware circolanti, classificati in modo corretto, e completi di tutte quelle informazioni accessorie che possono essere utili nell'attività di ricerca.

Impatti

- Il raggiungimento degli obiettivi di ricerca di questa articolazione comporterà benefici per tutti gli ambiti del sistema Paese che necessitano di protezione: maggiore protezione alle infrastrutture critiche, ai cittadini nella protezione dei loro dati e delle loro proprietà (auto a guida autonoma, domotica, dispositivi medicali), al mondo industriale.
- Un Paese che abbia sviluppato capacità di difesa attiva dagli incidenti informatici, capacità di compiere attività di intelligence per il contrasto al cybercrime e al cyberterrorism e di produrre evidenza per l'intera attività forense che segue l'incidente, è un Paese che ha una maggiore capacità di difesa rispetto alle aggressioni di natura criminale, terroristica e militare.
- Migliorare le tecniche di incident response produce benefici nelle organizzazioni che includono un SOC in termini di riduzione del rischio cyber sia come probabilità di accadimento degli incidenti informatici sia come impatto.

Key Performance Indicators

- Sviluppo di sistemi e linguaggi che implementano i metodi proposti, messi a disposizione della comunità scientifica.
- Composizione di adeguati dataset e diffusione della cultura sperimentale nella comunità, con condivisione dei dataset, dei package sperimentali e delle repliche sperimentali.
- Capacità delle organizzazioni di identificare, rilevare, analizzare e gestire gli incidenti informatici.
- Capacità delle organizzazioni di ridurre il tempo di esecuzione delle fasi dell'*incident response.*
- Quantità di informazioni acquisibile attraverso tecniche di cyber intelligence su specifici target.
- Pubblicazioni ad alto impatto nella comunità scientifica e iniziative imprenditoriali nel settore (spin-off, start-up).

Articolazione 2. Sicurezza dei sistemi cyber-fisici e delle infrastrutture di rete

La nostra società dipende ormai massicciamente da servizi erogati da sistemi digitali interconnessi tramite infrastrutture di comunicazione sempre più pervasive. L'evoluzione della tecnologica microelettronica, delle telecomunicazioni e dei sistemi software va però di pari passo con l'incremento delle vulnerabilità ad attacchi informatici presenti ai vari livelli e nei vari ambiti.

La crescente e sempre più capillare tendenza all'uso di tecnologie informatiche su dispositivi che tradizionalmente erano meccanici o comunque disconnessi spinge verso un sempre più massiccio impiego dei cosiddetti *sistemi cyber-fisici* negli ambiti più disparati, quali, a titolo di esempio, il monitoraggio, la gestione e la protezione di infrastrutture critiche, i trasporti (su gomma, su rotaia o aerei, con o senza pilota umano), le applicazioni mediche e biomedicali, le tecnologie assistive per agevolare e supportare disabili e persone con fragilità diverse.

La trasformazione digitale ha anche portato a perdere completamente il concetto di perimetro fisico in *ambito industriale* a causa dell'impiego sistematico di dispositivi IoT, di dispositivi mobili e di collegamenti a distanza. Ciò ha avuto il duplice effetto, da un lato, di far coincidere, di fatto, gli ambienti di *Information Technology* (IT) con quelli di *Operation Technology* (OT) e, dall'altro, di portare sempre più l'intera catena di approvvigionamento, la "supply chain", all'interno del perimetro aziendale. Le conseguenze in termini di security, safety e privacy sono del tutto evidenti.

Le *infrastrutture di rete e di storage* costituiscono la tecnologia abilitante della maggior parte delle moderne applicazioni digitali, intrinsecamente basate su forme - efficienti e regolamentate - di condivisione di informazioni. All'interno di queste, particolare attenzione va data a tecnologie diverse, che includono, tra l'altro, le software-defined network, le content-delivery network, le soluzioni di edge e fog computing e tutte quelle cloud-based. A queste, vanno aggiunte le nuove infrastrutture per le *comunicazioni mobili attuali e di prossima generazione* (5G e 6G), le cui prestazioni fanno da prologo alla progettazione di un'enorme varietà di nuovi servizi digitali, grazie alle garanzie di latenza e banda, non disponibili nelle attuali reti 4G. L'integrazione delle reti 5G e 6G con dispositivi di tipo IoT sempre più pervasivi daranno vita a quella che viene ormai chiamata la IoE, "Internet of Everything", con un conseguente incremento, sino a oggi inimmaginabile, della superficie di attacco.

In tutti questi ambiti occorrono investimenti in ricerca per trovare soluzioni in grado di coniugare al contempo aspetti di security, safety e privacy, garantendo le necessarie compatibilità con i vincoli di natura economica. Nel seguito consideriamo quattro obiettivi strategici da raggiungere per garantire usi sicuri di reti e servizi:

A. **Security, safety e privacy nei sistemi cyber-fisici**
B. **Security, safety e privacy in ambito industrial**
C. **Security e privacy nelle infrastrutture di rete e di storage**
D. **Security e privacy per comunicazioni mobili (5G e 6G)**

Obiettivi

A. Security, safety e privacy nei sistemi cyber-fisici

In questo contesto occorre considerare due dimensioni necessariamente complementari: quella prettamente tecnologica e quella inter- e multi-disciplinare.

Gli obiettivi tecnologici da perseguire nello s*viluppo di approcci, metodologie e strumenti per progettare e realizzare sistemi cyber-fisici sicuri* sono i seguenti:

- applicazione sistematica dei principi di *safety-*, *security-* e *privacy-by-design* e definizione di metodologie e standard in grado di garantire congiuntamente proprietà di safety e di security;
- possibilità di garantire la privacy dei dati di sensore fin dall'acquisizione stabilendo schemi di protezione "punto-punto" dell'identità dei nodi anche in presenza di indirizzi statici e pubblici come quelli IPv6.
- misurabilità delle proprietà di sicurezza per le varie componenti e per l'intero sistema, non solo a fine produzione, ma anche sul campo e a seguito di operazioni di manutenzione, aggiornamento e riconfigurazione e disponibilità di strumenti di monitoraggio e attivazione (semi)automatica di eventuali contromisure in caso di attacco;
- possibilità di supportare differenti modelli di programmazione e di modelli computazionali, nonché modelli di sicurezza in grado di tenere conto della natura eterogenea dei sistemi implementati.

Relativamente agli *aspetti inter- e multi-disciplinari* occorre invece perseguire obiettivi quali:

- piena verificabilità della coerenza delle operazioni di trattamento di dati personali con le leggi via via vigenti, tenendo conto che spesso i dati vengono "fusi" o combinati con altri dati per poi pseudonimizzarli o arricchirli o per estrarre dati aggregati;
- piena consapevolezza della eterogeneità dei livelli di trust dei vari gruppi di utenti, che possono essere soggetti a dinamiche e norme sociali le più svariate e modificabili nel tempo;
- definizione chiara delle responsabilità condivise tra i vari operatori coinvolti (ad esempio, il modello shared responsibility derivato dal cloud), anche attraverso la definizione di opportuni strumenti per gestire poliche e implementare meccanismi di sicurezza adatti ai contesti operativi e/o per utenti specifici.

B. Security, safety e privacy in ambito industriale

In questo ambito gli obiettivi da perseguire sono principalmente i seguenti:

- *Protezione della proprietà intellettuale e garanzia del prodotto*. Occorre sviluppare soluzioni che permettano di proteggere, in modo semplice ed efficiente, la proprietà intellettuale dei processi di produzione e dei prodotti immessi sul mercato ma anche di identificare, in modo non modificabile, la sorgente e lo stato dei propri prodotti stessi. Nel caso in cui questi ultimi non siano prodotti finiti, ma semi-lavorati o componenti, occorre identificare soluzioni in grado di garantire e rendere accessibile la cosiddetta *chain of identity*.
- *Messa in sicurezza dell'intera filiera OT*: l'estensione della convergenza tra IT e OT a tutta la catena di fornitura richiede la disponibilità di soluzioni in grado di condividere, in modo certificato e sicuro, tra tutti gli attori della catena stessa, un insieme sempre più vasto e articolato di dati sensibili (da un punto di vista industriale), provenienti dalla catena di progettazione, produzione, collaudo e dismissione dei prodotti.
- *Protezione dei siti di produzione*: occorre sviluppare metodologie e soluzioni in grado di garantire la possibilità, in caso di estreme emergenze, di cancellare, in tempi compatibili con la velocità della minaccia, tutti i dati presenti all'interno di un determinato sito di produzione, garantendo la completa e pronta ri-inizializzazione dell'impianto a minaccia conclusa.

C. Security e privacy nelle infrastrutture di rete e di storage

In questo ambito gli obiettivi da perseguire sono principalmente i seguenti:

- *Contrasto alle attività di sabotaggio.* Attività malevole di tipo Denial of Service sono in continua crescita, in particolare nei confronti di sistemi e infrastrutture critiche (energia, controllo traffico, finanza, Internet stessa), anche grazie alla pubblica diffusione di soluzioni di attacco "chiavi in mano", ed hanno le origini e gli obiettivi più svariati, dal terrorismo, alla competizione sleale fino al conflitto più o meno latente tra soggetti statuali (cyberwar).
- *Potenziamento delle capacità di difesa, contenimento e reazione agli attacchi.* Questo va perseguito tenendo conto dei problemi di scalabilità dovuti all'estrema difficoltà di implementare controlli e politiche di ispezione e di filtraggio del traffico a livello centralizzato, e quindi analizzando un numero limitato di punti strategici della rete, in ragione dei volumi di traffico coinvolti, delle normative relative al roaming, dei limiti tecnologici degli attuali apparati e delle soluzioni di security enforcement (Next Generation firewalls, Intrusion & anomaly detectors etc.).
- *Aumento della centralizzazione delle strategie di difesa.* Questo obiettivo va perseguito a livello dei grandi hub di concentrazione e interscambio del traffico, ma bisogna anche tenere conto della decentralizzazione, ovvero dello spostamento del focus della sicurezza/protezione verso la periferia della rete in maggiore prossimità delle risorse da proteggere in accordo a una logica di distribuzione delle strategie di difesa.
- *Automazione di azioni per garantire adeguati livelli di sicurezza, affidabilità e disponibilità.* Questo obiettivo si riferisce alla protezione di quelle infrastrutture critiche che sono monitorate, gestite o controllate tramite sistemi informatici e telematici. Tecniche di Intelligenza Artificiale possono essere usate per analizzare elevatissimi volumi di dati, per correlare e interpretare eventi e per intercettare/rispondere adeguatamente agli attacchi.
- *Integrazione dei diversi sistemi a supporto della sicurezza.* Sistemi quali firewall, IDS, IPS, antivirus etc. sono spesso forniti da diversi produttori, ognuno con specifiche soluzioni e caratteristiche "proprietarie". Questi non debbono più operare in maniera indipendente, in accordo a una logica "a silos", ma debbono cooperare scambiandosi dati in una logica di piena armonizzazione.

D. Security e privacy per comunicazioni mobili (5G e 6G)

In questo ambito gli obiettivi da perseguire sono principalmente i seguenti:

- *Cybersecurity e privacy in sistemi di comunicazione mobile di ultimissima generazione.* Questo obiettivo concerne l'analisi delle soluzioni di sicurezza e privacy specifiche per 5G, 6G e successive generazioni, nonché il progetto di soluzioni innovative sia a livello tecnologico sia a livello crittografico e protocollare. L'area di azione sarà principalmente riferita alle soluzioni specificate, o in fasi di specifica, nel contesto delle attività di standardizzazione 3GPP e della relativa architettura di sicurezza. Oltre alle attività di identificazione di attacchi e vulnerabilità, vanno considerate soluzioni innovative classificabili nel contesto degli attuali sei domini di sicurezza standardizzati (*network access*, *network domain*, *user domain*, *application domain*, *service-based architecture domain*, *visibility and configuration*), ma anche quelle relativi ad aspetti emergenti quali, ad esempio, *localization security*, integrità dei segnali, *location privacy*, rilevamento di "*fake*" *base station*, *jamming detection/prevention*, *downgrade/bid-down*.
- *Cybersecurity delle infrastrutture per sistemi di comunicazione mobile di ultimissima generazione.* Questo obiettivo è orientato alle problematiche di sicurezza relative all'infrastruttura tecnologica alla base dei protocolli di rete mobile 5G, 6G e successive generazioni per fornire le garanzie di affidabilità e disponibilità che tali sistemi - nel loro ruolo di infrastrutture critiche per il Paese - devono avere. Va garantita, da una parte, attraverso tecniche di *waveform design* e gestione avanzata dello spettro, la sicurezza dell'interfaccia radio relativamente ad attacchi su larga scala atti a minare la disponibilità dell'infrastruttura radio (DDoS, IoT botnet, etc) e, dall'altra, la sicurezza e l'affidabilità delle piattaforme di softwarizzazione della rete (NFV, SDN, slicing, etc). Per questo sono necessarie soluzioni tecniche di *hardening* dell'infrastruttura, soluzioni di monitoraggio dello spettro e *continuous assessment*, analisi delle problematiche emergenti dal considerevole allargamento della superficie di attacco e dalla necessità di coesistenza ed integrazione di molteplici stakeholder e differenti domini tecnologici.
- *Cybersecurity assurance per sistemi di comunicazione mobile di ultimissima generazione.* Questo obiettivo si riferisce alla produzione di metodologie, linee guida e framework per la security assurance dei più moderni sistemi di comunicazione mobile (valutazione, verifica, test, monitoraggio, etc). Alcuni obiettivi particolarmente innovativi e sfidanti sono i seguenti: (i) definizione di metodologie e soluzioni tecnologiche per l'analisi della sicurezza sull'interfaccia radio per l'analisi sia a livello di segnale sia a livello protocollare; (ii) definizione di metodologie di hardware security test specifiche per sistemi e dispositivi di comunicazione mobile; (iii) sviluppo di tecniche per la verifica della correttezza delle implementazioni dei protocolli e l'assenza di vulnerabilità indotte da queste; (iv) sistematizzazione della security assurance per sistemi di comunicazione mobile di ultimissima generazione, con particolare attenzione alla standardizzazione in corso nel contesto 3GPP (SCAS) e alle metodologie di valutazione e test promosse da consorzi e comitati 5G (es. GSMA/NESAS); definizione di metodologie di analisi di vulnerabilità e penetration test specificatamente orientate a sistemi e servizi di comunicazione mobile e associate a metodologie e piattaforme per il training in grado di garantire completa integrità protocollare degli attacchi fino al livello fisico (5G cyber-range).

Impatti

Gli impatti delle linee di ricerca qui delineate sono enormi in quanto strettamente legati alla già discussa pervasività dei sistemi cyber-fisici. Risulta evidente che essi riguardano le tecnologie di supporto ai sistemi digitali, e le persone fisiche e giuridiche che vi interagiscono e, in particolare, garantiscono:

- Incremento dell'utilizzo di sistemi cyber-fisici, anche intelligenti.
- Indipendenza dell'utilizzo di sistemi cyber-fisici dal grado di istruzione o attitudine alla tecnologia degli individui.
- Modernizzazione tecnologica della società, con aumento del mercato per dispositivi cyber-fisici nonché delle applicazioni di infrastrutture di rete.
- Riduzione dell'errore umano nell'utilizzo di sistemi cyber-fisici.
- Miglioramento della consapevolezza generale dei benefici della tecnologia esposta tramite sistemi cyber-fisici e infrastrutture di rete.
- Aumento della resilienza del sistema industriale verso attacchi informatici di varia natura e portata.

- Aumento della resilienza della società nei confronti di attività malevola finalizzata all'esfiltrazione di dati personali da sistemi cyber-fisici di vasto utilizzo.

Key Performance Indicators

- Definizione di approcci interdisciplinari alla risoluzione dei problemi di cybersecurity e privacy nei domini applicativi più diversi.
- Aumento della fiducia sociale nelle tecnologie informatiche.
- Aumento delle applicazioni sicure delle infrastrutture di rete.
- Aumento della resilienza del sistema industriale.
- Prototipazione di comunicazioni mobili di generazione oltre 5G.
- Pubblicazioni ad alto impatto nella comunità scientifica e iniziative imprenditoriali nel settore (spin-off, start-up).

Articolazione 3. Tecniche e metodologie per la protezione delle risorse

I fabbisogni di protezione che coinvolgono i più recenti scenari caratterizzati dall'uso delle tecnologie digitali richiedono investimenti in diverse aree tematiche e tecnologie abilitanti, con approcci spesso necessariamente trasversali e multidisciplinari che coinvolgono la crittografia, il controllo degli accessi, l'intelligenza artificiale e gli strumenti di protezione dell'hardware.

La crittografia fornisce strumenti e metodologie per garantire confidenzialità, autenticazione, integrità, non-ripudio, e anonimato. Un semplice personal computer o anche un dispositivo con minori risorse computazionali possono eseguire primitive crittografiche di tale complessità da rendere praticamente impossibile la crittoanalisi, anche utilizzando il lavoro coordinato dei moderni super-computer.

Di fronte a cyber attacchi sempre più sofisticati e a tecniche d'attacco che possono ricorrere a tecnologie nuove e dirompenti, la protezione dei dati e più in generale delle risorse presenti nel cyberspazio attraverso il controllo granulare dell'accesso agli stessi, è diventato uno dei temi centrali per la cybersecurity. Inoltre, con l'entrata in vigore del General Data Protection Regulation (GDPR) dell'Unione Europea e alla luce dei potenziali danni causati da furti e perdite di dati, i rischi, sia finanziari sia d'immagine, a essa correlati diventano un fattore di primaria importanza per la vita di qualsiasi organizzazione.

L'Intelligenza Artificiale (IA) e più in generale le tecnologie con capacità di apprendimento, ragionamento e decisione semi-autonoma stanno assumendo un ruolo sempre più strategico nella sicurezza, in particolare per quanto riguarda il supporto decisionale nelle strategie di difesa e reazione. Infatti, l'introduzione di sistemi basati sull'Intelligenza Artificiale per affiancare e sostituire ove possibile gli esperti diventa l'unica soluzione percorribile per trattare elevatissimi volumi di dati e correlare e interpretare eventi alla velocità necessaria a rispondere adeguatamente ad attività ostili.

L'esigenza di "protezione" delle infrastrutture hardware, ribadita peraltro anche dalle recenti normative sia comunitarie sia nazionali, richiede oggi significativi investimenti in termini di ricerca, al fine di tendere a ridurre la marginalità sia tecnologica sia economica del settore rispetto ai player internazionali, arrivando con urgenza ad avere una "tecnologia nazionale".

Tenendo presente queste considerazioni, nel seguito della descrizione di questa articolazione analizzeremo quattro dei principali approcci alla difesa cyber assieme agli obiettivi da perseguire per migliorare la capacità di difesa del sistema Paese:

A. **Crittografia**
B. **Autenticazione, Regolamentazione dell'Accesso e Utilizzo dei Dati**
C. **IA per Cybersecurity e Cybersecurity per IA**

D. Hardware Security e Hardware-based Security

Obiettivi

A. Crittografia

I sistemi più utilizzati per la firma digitale, crittografia a chiave pubblica, accordo su chiavi, forward secrecy, si basano sull'ipotesi che alcuni problemi computazionali, quali la fattorizzazione e il calcolo del logaritmo discreto, siano difficili da risolvere e richiedano tempi e risorse enormi per la loro soluzione. La possibilità di risolvere tali problemi in tempi computazionalmente accettabili usando la tecnologia di calcolo quantistica ha avuto un profondo impatto sulla ricerca crittografica e ha posto il problema della sostituzione delle infrastrutture a chiave pubblica esistenti e della definizione di nuovi crittosistemi "quantum-resistenti". I temi di ricerca della crittografia quantum-resistente non vanno confusi con quelli della crittografia quantistica propriamente detta. Quest'ultima sfrutta proprietà di entaglement dei bit quantistici per costruire primitive crittografiche, come ad esempio l'accordo su chiavi (quantum key exchange) che già oggi viene usato in sistemi di telecomunicazione punto-punto. La *cifratura omomorfa* è una tecnica che permette di processare i dati cifrati senza doverli prima decifrare e quindi di delegare le computazioni sui dati cifrati senza dare l'accesso ai dati in chiaro. I dati possono essere cifrati e inviati anche a servizi di cloud commerciali per poter essere poi elaborati sempre in forma cifrata. Uno scenario di interesse è quello della salute, in cui occorre superare le problematiche legate alla privacy della gestione dei dati medici. In molti settori vengono utilizzati dispositivi interconnessi ma con molte limitazioni, che comunicano per il raggiungimento di un obiettivo, ma la maggioranza degli algoritmi crittografici, progettati per ambienti desktop o server, non sono utilizzabili in questi casi. Alcune applicazioni quali le votazioni elettroniche o le transazioni economiche richiedono confidenzialità e anonimato, ma anche correttezza e verificabilità e in alcuni casi necessitano di un consenso di comunità sulle proprietà di dati condivisi in assenza di un'autorità fidata. Nell'area della crittografia è necessario capire i limiti e le possibilità delle soluzioni disponibili per poter poi fornire e analizzare nuove proposte; in particolare è importante considerare:

- Nuove primitive crittografiche in grado di resistere ad attacchi basati sull'uso di computer quantistici che, quando saranno disponibili su larga scala, renderanno vulnerabili schemi crittografici molto diffusi. Il processo di standardizzazione del NIST per crittosistemi quantum-resistenti è giunto al 22 luglio 2020 a selezionare 15 candidati al termine della fase 2. Le fasi successive dovrebbero completarsi nel 2022. Gli standard crittografici dovranno essere aggiornati e poi occorrerà una rapida transizione per la loro adozione da parte dei governi e del mondo industriale e si dovrà definire una effettiva costruzione di schemi di distribuzione di chiavi anche nell'ambito della crittografia quantistica.
- Cifrature omomorfe efficienti. Ne trarranno giovamento i protocolli per delegare la computazione sui dati cifrati preservando la privacy.
- Primitive crittografiche leggere (lightweight) come cifrari a blocchi e funzioni hash e protocolli leggeri per l'autenticazione e la cifratura autenticata, per la sicurezza dei dispositivi interconnessi che hanno risorse computazionali e di memoria limitate.
- Progetto e analisi di protocolli sicuri finalizzati a risolvere specifici problemi che coinvolgono più entità (*secure multiparty computation*). È rilevante anche la costruzione e analisi di elementi costitutivi utili come *zero-knowledge*, *secret sharing*, *oblivious transfer*.
- Progetto e analisi di protocolli di consenso per registri distribuiti che siano adatti a una vasta gamma di applicazioni, e che garantiscano efficienza computazionale e risparmio energetico.

B. Autenticazione, Regolamentazione dell'Accesso e Utilizzo dei Dati

L'enorme quantità di dati che oggi devono essere memorizzati ed elaborati in modo efficace ed efficiente introduce il bisogno di sviluppare piattaforme di elaborazione scalabili, efficienti e affidabili. Per questo, spesso i dati vengono ceduti in gestione a terze parti che offrono disponibilità di un accesso continuo, bassi costi, e disponibilità di servizi

elastici di archiviazione ed elaborazione. Nonostante questi vantaggi, la raccolta, memorizzazione, elaborazione e condivisione di dati tramite questi servizi pone dei seri interrogativi su confidenzialità e integrità dei dati stessi e delle elaborazioni. A tale scopo sono sempre più necessarie, oltre ad approcci specifici per il controllo dell'integrità, politiche di controllo dell'accesso che tengano conto di accordi specifici tra le parti e che devono essere basati su modelli e meccanismi flessibili. Attualmente, esiste un chiaro conflitto di obiettivi: i dati dovrebbero essere suddivisi in compartimenti stagni al fine di garantirne la protezione e al contempo condivisi nei processi inter-organizzativi quali le catene di fornitura. Sebbene rappresentazione e composizione di politiche di controllo dell'accesso siano state studiate da lungo tempo e linguaggi di politiche come XACML siano disponibili ormai da anni, l'applicazione automatica di politiche multiple su modelli di dati eterogenei è ancora un problema aperto. Ulteriori sfide sono introdotte dalla diffusione del fenomeno BYOD (Bring Your Own Device), che portano asset aziendali e dati e applicazioni personali dell'utente a convivere sugli stessi dispositivi, esponendo le organizzazioni coinvolte a maggiori rischi di sicurezza e gli utenti a rischi legati a violazioni della loro privacy.

Il problema del controllo dell'accesso è strettamente legato a quello dell'autenticazione, considerato che occorrono tecniche sofisticate, sicure e affidabili di identificazione dei soggetti e degli asset a cui le politiche si applicano. L'autenticazione è al centro delle strategie di sicurezza di qualsiasi organizzazione, e, al fine di proteggere i dati contenuti nel suo perimetro e un qualsiasi meccanismo di controllo accessi, richiede di procedere preliminarmente all'identificazione dei soggetti coinvolti. Purtroppo, anche gli schemi di identificazione più sofisticati quali quelli *knowledge-*, *token-* o *certificate*-based possono presentare vulnerabilità, in quanto le credenziali possono essere acquisite in maniera fraudolenta da soggetti terzi, così come i certificati digitali. Bisogna intensificare la ricerca per raggiungere i seguenti obiettivi:

- Superare l'approccio classico che concede l'accesso alle risorse in base al ruolo del soggetto che ne fa richiesta e sperimentare modelli più flessibili in cui a risorse e soggetti venga associata una serie di attributi e la decisione sull'accesso venga presa in base a una valutazione comparativa degli attributi della risorsa e del soggetto anche affiancando al tradizionale controllo dell'accesso di tipo preventivo meccanismi basati su rilevamento di comportamenti difformi alle politiche stabilite e meccanismi opportuni di sanzione e premio.
- Sviluppare logiche di controllo accesso in cui (i) i diritti di accesso per un soggetto cambiano nel tempo, secondo uno specifico algoritmo capace di adattarsi a variazioni di tipo contestuale, (ii) le regole di controllo dell'accesso cambiano in base al fattore di rischio e al livello di trust richiesto, eventualmente utilizzando tecniche di apprendimento automatico per identificare le minacce in tempo reale.
- Sviluppare tecniche per il controllo di accesso nei sistemi decentralizzati anche per evitare modifiche manuali delle politiche di controllo in settori dove la suddivisione dei compiti organizzativi richiede a più soggetti di accedere ai dati di proprietà di molte organizzazioni diverse all'interno dello stesso processo inter-organizzativo.
- Individuare caratteristiche fisiche o comportamentali in grado di soddisfare i vincoli di accettabilità e affidabilità richiesti dalle tecniche di identificazione biometriche e sviluppare nuove soluzioni multi-modali o multi-biometriche, basate sulla creazione di crittosistemi biometrici "senza chiave" (o meglio, con chiavi generate a partire da segnali biometrici).
- Combinare tecniche di *sandboxing* e crittografia per gestire dispositivi sui quali coesistono dati personali e aziendali e garantire che le politiche di separazione tra i due "domini" siano efficacemente controllate.
- Sviluppare modelli e politiche di controllo dell'accesso, integrabili nei sistemi esistenti, in grado di esprimere requisiti di privacy che regolamentano come memorizzare, condividere ed elaborare informazioni in conformità a normative tipo GDPR.
- Sviluppare tecniche in grado di garantire la sicurezza e la protezione dei dati usati in elaborazioni che prevedano il coinvolgimento di diverse parti; tali tecniche devono permettere di rappresentare in modo semplice ed espressivo i diversi privilegi di accesso delle parti coinvolte e devono bilanciare le necessità di condivisione e di protezione dell'informazione.

- Sviluppare soluzioni applicabili in scenari che richiedono elaborazioni complesse su enormi quantità di dati che siano in grado di garantire che il risultato di elaborazioni distribuite sia integro e affidabile.

C. IA per Cybersecurity e Cybersecurity per IA

I più recenti ed affermati prodotti e servizi di sicurezza (sistemi antivirus, SIEM) sono abilitati da alcune tecniche di intelligenza artificiale, ma i risultati sono lungi dall'essere consolidati. Con adeguati investimenti in ricerca, l'utilizzo di algoritmi e tecniche di Intelligenza Artificiale (IA) potrebbe supportare la sicurezza a diversi livelli, a partire dall'identificazione totalmente automatica delle situazioni anomale potenzialmente pericolose, riconoscendo gli eventi, che collettivamente possono evidenziare una deviazione sospetta rispetto ai comportamenti che caratterizzano la normale operatività degli obiettivi da proteggere. A tale proposito, la capacità di "apprendere" delle soluzioni di IA diventa un elemento difensivo strategico, specialmente se associati a feedback umani o semi-automatizzati nella logica del *reinforcement learning*. Tali soluzioni hanno anche il vantaggio di auto-aggiornarsi continuativamente, costruendo nuova conoscenza a partire dalle esperienze precedenti (*re-training*) in modo da imparare a identificare correttamente anche le nuove minacce man mano che queste si presentano.

L'importanza strategica dei sistemi di IA in ambito cybersecurity li rende un obiettivo sensibile ad attacchi mirati a minarne la stabilità e l'efficacia. Tali minacce devono essere contrastate attraverso nuovi modelli di difesa non ancora noti in ambito cybersecurity. I casi di attacco *adversarial* più noti coinvolgono algoritmi di classificazione e riconoscimento video che vengono ingannati introducendo opportuno "rumore" oppure sistemi di *gaming* strategico estremamente potenti che vengono ingannati da particolari comportamenti di gioco che difficilmente influenzerebbero un avversario umano. Anche veicoli autonomi o sistemi robotici in grado di operare bene in condizioni normali possono essere indotti a fallire sfruttando opportune vulnerabilità delle componenti di *deep learning* che ne caratterizzano il comportamento. Ad esempio, gli algoritmi di apprendimento automatico che operano in condizioni non-stazionarie vengono ri-addestrati su dati collezionati durante la fase operativa per seguire i cambiamenti della distribuzione statistica dei dati di ingresso. In questo scenario, un attaccante può contaminare i dati di addestramento iniettando campioni costruiti ad hoc per compromettere l'intero processo di apprendimento. Per questo è necessario perseguire molteplici obiettivi:

- Sviluppare nuove soluzioni di difesa da attacchi di tipo avversariale, in grado di partire dalla conoscenza profonda dei meccanismi di base delle soluzioni di IA per contrastarne l'abuso.
- Automatizzare il più possibile tutte le azioni tese a garantire un adeguato livello di sicurezza, affidabilità e disponibilità dei sistemi informatici e telematici attraverso l'introduzione di intelligenza algoritmica e capacità di analisi evoluta nelle attività di monitoraggio, gestione o controllo, in modo da superare i limiti tecnologici attraverso una migliore visione e comprensione dei fenomeni (la cosiddetta *consapevolezza situazionale*).
- Acquisire maggiore conoscenza e controllo delle proprietà di robustezza delle caratteristiche chiave degli algoritmi di apprendimento automatico (ad esempio, le superfici di separazione tra categorie dei classificatori) contro attacchi di adversarial IA specificatamente mirati a modificarle in maniera fraudolenta, e sviluppare contromisure sistematiche adatte a costruire e progettare sistemi di apprendimento automatico più sicuri.
- Sviluppare tecniche di IA per la definizione di politiche di controllo dell'accesso adattive, e per *anomaly detection*, *fake indentity detection* e individuazione di preferenze di privacy.

D. Hardware security e Hardware-based security

Due sono le direttive principali lungo le quali orientare la ricerca, appartenenti a quelle che in letteratura vengono identificate rispettivamente come *hardware security* e *hardware-based security*.

Nell'ambito della hardware security, occorre mettere in campo le risorse necessarie per la progettazione e la realizzazione delle cosiddette *architetture nazionali tolleranti le vulnerabilità*, in grado di garantire livelli di sicurezza predefiniti, anche in sistemi che contengono dispositivi hardware o che eseguono applicativi software, con vulnerabilità di diversa natura, note o non ancora rivelate. Le soluzioni proposte, da sviluppare secondo i paradigmi

della *security-by-design*, devono essere in grado di fornire livelli di sicurezza variabili e adattabili alle diverse criticità dei sistemi rispetto allo specifico dominio applicativo. Il controllo del Paese su queste architetture deve necessariamente essere completo: nell'allestimento di una produzione "nazionale" occorrerà pertanto rendere fidata (e quindi sviluppata in ambienti adeguatamente protetti) l'intera filiera, che va dalla progettazione al processo di produzione, al collaudo, alla certificazione, all'installazione, alla manutenzione, agli aggiornamenti e alla dismissione. In ciascuna fase sarà anche necessario garantire adeguati livelli di fiducia nelle persone coinvolte, negli strumenti di ausilio alla progettazione impiegati e nelle eventuali terze parti reperite a qualsiasi titolo sul mercato estero. Nell'ambito, invece, della hardware-based security, occorre mettere in campo le risorse necessarie per progettare e sviluppare soluzioni integrate in grado di offrire *root of trust* per applicazioni basate su dispositivi IoT e Industrial IoT.

Le soluzioni proposte dovranno, tra l'altro, perseguire i seguenti obiettivi:

- essere in grado di soddisfare la piena aderenza a standard internazionali presenti, quali, a titolo di esempio, TPM (Trusted Platform Module), TEE (Trusted Execution Environments) e futuri;
- essere compatibili con i vincoli imposti dai diversi ambienti applicativi, ad esempio in termini di costi, limitatezza delle capacità computazionali, limitatezza della banda per le comunicazioni, limitatezza nella accessibilità fisica, requisiti di safety, etc.;
- essere adattabili ai domini applicativi più diversi, dalla domotica all'healthcare, dalle applicazioni per smart-city all'ambito industriale;
- poter integrare, sempre nel rispetto dei vincoli, soluzioni di identificazione univoca dei singoli dispositivi, basate tipicamente su PUF (Physically Unclonable Function).

Particolare attenzione va attribuita a soluzioni che, pur essendo basate su approcci di tipo open source, siano poi in grado di essere adattate e personalizzate con facilità per rispondere a specifiche esigenze di sicurezza e riservatezza.

Impatti

Il raggiungimento degli obiettivi di ricerca di questa articolazione comporterà benefici per tutti gli ambiti del sistema Paese che necessitano di tecniche e metodologie di protezione attraverso la formulazione di un approccio alla sicurezza olistico, coordinato e multi-dimensionale.

Lo sviluppo delle conoscenze delle tecniche e delle metodologie crittografiche permetterà una maggiore garanzia di confidenzialità, autenticazione, integrità, non-ripudio, e anonimato e una conseguente ricaduta in ambito industriale, militare e civile.

L'introduzione di tecniche di IA a supporto della cybersecurity, unita a una logica di cooperazione e interscambio della conoscenza, consentirà ai moderni sistemi di sicurezza di raccogliere e condividere delle informazioni costruendo una conoscenza collettiva sedimentata dalla quale attingere in logica inferenziale per elaborare autonomamente le risposte più adatte alle situazioni che possono presentarsi e quindi velocizzare e sistematizzare la correlazione di determinati eventi con potenziali incidenti. Per quanto riguarda gli attacchi specifici ai sistemi e ai modelli IA (adversarial IA), la conseguenza più immediata sarà lo sviluppo di metodologie che permettano di valutare la sicurezza degli algoritmi di apprendimento automatico, simulando in anticipo e in modo proattivo i potenziali attacchi e le loro conseguenze sulle prestazioni dei sistemi intelligenti. Queste metodologie dovrebbero poter suggerire come mitigare l'impatto di alcuni attacchi sui modelli considerati, aumentandone la robustezza.

In ambito regolamentazione dell'accesso e utilizzo dei dati, il processo di evoluzione dalla logica di controllo accessi tradizionale basata su tecnologie *single sign on* e autenticazione a due fattori verso nuovi modelli estremamente più flessibili ed adattativi, supportati da schemi *attribute-based* e da ambienti di enforcement dinamico e scalabile, renderà sempre più trasparenti le tecnologie di sicurezza minimizzandone l'impatto sull'utente finale. Con le nuove tecnologie di gestione accesso personalizzata, gli utenti non saranno più limitati dalla presenza di meccanismi e vincoli di sicurezza e il processo di identificazione dei soggetti e di soddisfacimento da parte loro delle richieste delle politiche di autorizzazione sarà automatizzato, offrendo un'esperienza d'uso più sicura e priva di fastidi.

In ambito hardware security e hardware-based security, i risultati della ricerca permetteranno di incrementare il ruolo della filiera all'interno del panorama economico non solo nazionale e di ridurre la marginalità sia tecnologica sia economica del settore rispetto ai player internazionali, arrivando ad avere una "tecnologia nazionale" che garantisca il controllo completo delle tecnologie ritenute strategiche non solo per la sicurezza nazionale ma per l'intero sistema Paese. I risultati della ricerca saranno di supporto al decisore politico nella definizione di una strategia che permetta di decidere, per ciascuna categoria e sottocategoria di componenti e di tecnologie, quali siano quelle da sviluppare a livello nazionale e quali quelle che possano essere acquistate sul mercato estero. Le conoscenze e le competenze acquisite in questi ambiti potranno poi essere impiegate con profitto da tutti i laboratori pubblico/privati che dovranno essere attivati come supporto alle certificazioni attualmente in fase di definizione a livello sia comunitario sia nazionale.

Key Performance Indicators

- Sviluppo di nuovi schemi crittografici e modelli di controllo accessi;
- Sviluppo di nuovi approcci biometrici per l'autenticazione;
- Sviluppo di nuovi modelli e tecniche per la regolamentazione di accessi ai dati;
- Sviluppo di nuovi prodotti industriali basati sul consolidamento della ricerca;
- Registrazione di brevetti;
- Pubblicazioni ad alto impatto nella comunità scientifica e iniziative imprenditoriali nel settore (spin-off, start-up).

Articolazione 4. Sicurezza dei servizi al cittadino e alle imprese

Il futuro della nostra società dipende sempre più dalla possibilità di sfruttare l'enorme quantità di dati prodotti dai dispositivi digitali, nell'interesse della comunità dei cittadini. Difatti, usare tali dati è fondamentale per competere a livello globale e per garantire crescita economica. Una sfida importante che ci attende nei prossimi anni è quindi la definizione di modelli di dati e di sistemi digitali centrati sugli interessi *di cittadini e di imprese* relativamente ai quali la privacy e, più in generale, la tutela dell'utente siano posti al centro del processo di progettazione di un sistema informatico. Le istanze di questo scenario sono molteplici.

La prima istanza riguarda la definizione di sistemi e strumenti che consentano di *monitorare processi complessi garantendone la trasparenza.* Tutti i fenomeni riferiti come "italian sounding" rappresentano concorrenza sleale verso i nostri prodotti, con conseguenti sottrazioni di quote di mercato significative e danni d'immagine al Made in Italy; strumenti di monitoraggio e garanzia di filiera porterebbero benefici in molti settori del nostro Paese. Nel settore *agro-alimentare*, si è assistito, negli ultimi anni, a un cambiamento di atteggiamento dei consumatori che attribuiscono un'importanza sempre crescente a qualità, tipicità, origine ed eticità. Per sfruttare a pieno questa opportunità, è necessario *fornire certificazioni certe e sicure della merce italiana*, e questo implica trasparenza di tutta la filiera. Nella *moda* è essenziale tracciare, oltre alla provenienza dei tessuti, i luoghi di lavorazione e altre caratteristiche in termini di salubrità, sostenibilità ambientale e responsabilità sociale dell'impresa di produzione. Nel settore *farmaceutico* un tracciamento efficace dell'intero processo di produzione di un farmaco, dalla sperimentazione, al processo di approvazione, fino alla vendita, può portare benefici in termini di condivisione di informazioni e rapidità di produzione. Anche la *Pubblica Amministrazione* beneficerebbe di un sistema che permetta di tracciare e rendere disponibili identità digitali, capitoli di spesa, risorse finanziarie e pagamenti e consenta una maggiore consapevolezza per il cittadino.

La seconda istanza riguarda la definizione di strumenti per contrastare la diffusione di *notizie false* o, più in generale, la presenza di contenuti orientati alla *disinformazione* del cittadino, quali la diffusione di notizie inaccurate o comunque fuorvianti, pubblicate con lo scopo di provocare un danno all'interesse pubblico e/o per ottenere un profitto economico. Fenomeni di questo genere possono avere anche impatto negativo su diversi processi democratici, quali i processi elettorali, e su settori di vitale importanza, quali la sanità, l'istruzione, la finanza, etc. Questo problema è particolarmente complesso, in quanto il confine tra notizie false/fuorvianti e altri tipi di contenuto legittimi, ad esempio a carattere di satira o parodia, è spesso di difficile individuazione, e negli ultimi anni hanno avuto

impatti molto significativi a causa dell'amplificazione di notizie false, o fuorvianti, diffuse mediante gli online social media. Il problema è ancora più critico in situazioni di crisi, quali quella della recente epidemia di SARS-CoV-2, in cui la diffusione di informazioni sanitarie di provenienza non verificata può mettere a repentaglio la vita stessa delle persone.

Condivisione di informazioni, analisi dati, monitoraggio di processo e trasparenza portano significativi vantaggi nell'offerta di servizi ma rappresentano anche significative minacce alla privacy dei cittadini e alla loro possibilità di effettuare scelte informative consapevoli. Per questo, è necessario mettere i cittadini in grado di controllare i propri dati, decidere quando, con chi e con quali modalità condividere i propri dati ed essere informati relativamente alle fonti delle informazioni diffuse in rete. I temi elencati interessano molteplici campi di ricerca in ambito informatico; nel seguito descriveremo gli obiettivi da raggiungere per la realizzazione di una società centrata sui bisogni del cittadino che offra affidabilità e trasparenza nei servizi informatici:

A. **Trasparenza nel controllo di processi complessi**
B. **Affidabilità delle Fonti di Informazione e modelli di Trust**
C. **Privacy dei Dati**

Obiettivi

A. Trasparenza nel controllo di processi complessi

Questo obiettivo riguarda la definizione di sistemi e strumenti per il tracciamento di processi complessi che coinvolgono un alto numero di entità partecipanti in cui il livello di "fiducia" tra i partecipanti è basso se non inesistente. Tali sistemi consentiranno, ad esempio, di tracciare prodotti e materie prime con l'obiettivo di valorizzare i prodotti autentici italiani e di fornire alle nostre aziende un vantaggio competitivo nei mercati. La tecnologia basata su *Distributed Ledger (DL)*, ovvero sull'uso di *registri distribuiti*, di cui le blockchain rappresentano un'istanza, presenta aspetti promettenti per il conseguimento di questo obiettivo. Affinché tale metodologia acquisisca il livello di maturità necessario per supportare in modo efficace il controllo di processi complessi, occorre perseguire i seguenti obiettivi:

- *Integrazione di un DL nazionale* con ledger utilizzati da consorzi di imprese diverse. Lo scenario previsto è simile a quello accaduto per Internet, in cui reti di domini amministrativi autonomi sono state in seguito collegate tra di loro per formare la rete attuale. Analogamente, è opportuno integrare DL realizzati con tecniche diverse e gestiti da diversi consorzi, per *formare un Interledger*. Questa strutturazione sarebbe particolarmente utile in processi di tracciamento che coinvolgono dati provenienti da diverse filiere produttive. Un ulteriore obiettivo di ricerca sui DL riguarda la valutazione di modelli che definiscono diversi livelli di accessibilità ai DL da parte di varie classi di utenza, quali modelli *permissioned/permissionless, o private/public* in riferimento a scenari reali, anche per proporre modelli alternativi con funzionalità aggiuntive per un supporto efficace agli specifici casi d'uso.
- *Definizione di algoritmi e tecnologie che consentano di aumentare la scalabilità dei DL* che non sono ancora adeguati a supportare processi complessi che coinvolgono un numero di attori molto elevato. Per raggiungere un alto livello di scalabilità, garantendo al contempo sostenibilità energetica, è necessario definire nuovi e più efficienti algoritmi di consenso per i quali è richiesto lo sforzo congiunto di diversi ambiti di ricerca, quali quello degli algoritmi distribuiti, delle tecniche di incentivazione basate su teoria dei giochi, della crittografia. Più in generale, è auspicabile la definizione di strutture più complesse rispetto alla blockchain, che consentano un maggior livello di strutturazione dei dati tracciati.
- *Integrazione della tecnologia dei DL con quella dell'IoT* per tracciare diversi processi logistici che utilizzano dati rilevati da sensori, da sistemi *indossabili*, e in generale da dispositivi IoT. La possibilità di fornire a questi dispositivi un accesso autonomo ai DL per la registrazione di eventi e rivelazioni, senza alcun intervento umano, costituisce un altro elemento fondamentale per evitare la manipolazione dei dati e garantire un maggior livello di sicurezza del sistema.

- *Definizione di sistemi di tokenizzazione* per creare e distribuire token mediante DL che possono essere usati in diversi contesti quali *sistemi decentralizzati di protezione del diritto di autore,* in cui il diritto di fruizione dell'opera di ingegno sia frammentato in token multipli che possano essere scambiati autonomamente, oppure *sistemi per il frazionamento dei diritti su un bene,* ad esempio un diritto edificatorio o accessorio, in modo che sue diverse parti possano essere commercializzate separatamente. Per questo è necessario definire specifici modelli di produzione di token e tecniche per lo scambio e la loro custodia sicura, nonché *modelli di "rewarding"* volti a premiare comportamenti virtuosi degli utenti di un sistema.
- *Sicurezza dei processi di tracciamento.* L'efficacia dell'applicazione della tecnologia DL ai processi di tracciamento dipende anche da un'analisi accurata dei problemi di sicurezza dei DL stessi e dalla definizione di opportune contromisure. I problemi di sicurezza possono riguardare i diversi livelli dei sistemi quali, ad esempio, la vulnerabilità dei meccanismi crittografici, gli attacchi al livello della rete *peer to peer* sottostante (*replay*, *sybil*, *eclipse attack*, ...), la malleabilità delle transazioni registrate su DL, gli attacchi con quantum computer, le vulnerabilità nel codice degli *smart contract*, etc. Questo obiettivo necessita di molteplici competenze che vanno dalla crittografia alle tecniche formali per la specifica e la verifica degli smart contract, dall'analisi forense delle transazioni allo studio degli algoritmi distribuiti.

B. Affidabilità delle Fonti di Informazione e Modelli di Trust

Il tema della verifica dell'affidabilità delle fonti di informazione è un argomento complesso che coinvolge i ricercatori ma anche i cittadini che devono essere sensibilizzati in merito ai fenomeni complessi che li riguardano da vicino. La definizione di modelli e strumenti per la verifica delle fonti di informazione richiede uno sforzo congiunto in diversi campi di ricerca che vanno dalla cybersecurity all'analisi di grosse quantità di dati, supportata da strumenti di intelligenza artificiale, alla definizione di modelli di trust, fino all'attivazione di campagne di sensibilizzazione del cittadino rispetto al problema di un uso corretto e consapevole delle nuove tecnologie. Obiettivi di ricerca importanti sono:

- *Sviluppo di strumenti e piattaforme per la verifica della provenienza di informazioni diffuse su piattaforme digitali*. Tali strumenti dovranno mettere in grado il cittadino di verificare l'attendibilità delle informazioni reperite sulla rete. Scenari di interesse, in questo ambito, sono (i) *individuazione di informazioni prodotte e amplificate artificialmente da bot*, (ii) *verifica della validità di informazioni diffuse da influencer,* figure in grado di influenzare un gran numero di persone tramite la pubblicazione di opinioni su reti social, (iii) *tracciabilità della provenienza* di notizie provenienti da online social networks.
- *Sviluppo di strumenti e metodologie per garantire la trasparenza degli algoritmi* utilizzati per selezionare e personalizzare l'informazione diretta ai singoli utenti. Le raccomandazioni di beni di consumo/servizi proposti al cittadino sono spesso generate da algoritmi, frequentemente basati su tecniche di Intelligenza Artificiale, che non sono verificabili da parte della comunità. La tecnologia degli *smart contract,* codici pubblici e verificabili in quanto pubblicati su DL, costituisce una tecnologia di indubbio interesse in questo campo.
- *Attivazione di campagne di responsabilizzazione dell'utente* in merito ai contenuti fruiti attraverso reti digitali. Tali campagne dovranno essere supportate dallo studio e lo sviluppo di un insieme di strumenti (plugin browser, applicazioni per smartphone) di facile utilizzo, che consentano all'utente di interagire in modo immediato con i social media per verificare l'attendibilità delle fonti.
- *Definizione di linguaggi, sistemi e strumenti per la specifica di livelli di trust e reputation.*
- Questo tema riguarda la definizione di strumenti per l'individuazione di contatti affidabili all'interno di comunità virtuali ma anche l'affidabilità dei servizi forniti da entità sconosciute. Tali strumenti devono essere progettati in modo da divulgare solo le informazioni per le quali sia stato dato esplicito consenso, rispettando quindi i vincoli di privacy. In questo ambito, campi di ricerca importanti sono la ricerca di modelli per le relazioni sociali, l'analisi dei fattori che portano alla formazione del trust e della reputazione in ambiti virtuali, la definizione di sistemi di inferenza di livelli di trust. In questo contesto servono competenze di psicologia e sociologia.

C. Privacy dei Dati

Questo obiettivo riguarda la ricerca di strumenti e metodologie che consentano di garantire al cittadino alti livelli di privacy e, contemporaneamente, permettano di utilizzare i dati prodotti dalla comunità, opportunamente anonimizzati per la ricerca scientifica e per altri scopi che possano portare benefici alla collettività. Gli obiettivi primari sono:

- *Definizione di tecniche per la protezione dei dati* che possano garantire la privacy degli utenti, e consentire, al contempo, l'analisi di dati sensibili da parte di enti scientifici o imprese, nell'interesse della comunità. Si considerino, ad esempio, scenari in cui è importante garantire le esigenze di privacy del singolo cittadino e contemporaneamente utilizzare dati per obiettivi di salute pubblica, come nel caso della recente epidemia di SAR-COVID19. Temi di ricerca, in questo campo, riguardano l'individuazione di tecniche quali quella basata sul concetto di *differential privacy*, che hanno come obiettivo l'inserimento di "rumore" nei dati per evitare l'inferenza di dati sensibili e, allo stesso tempo, garantire risultati corretti delle analisi effettuate.
- *Garanzia di "Self-Sovereign Identity"* e cioè restituire al cittadino il controllo sulla propria identità, non più gestita in modo centralizzato, ma dai singoli individui in modo autonomo. Questo tema risulta rilevante rispetto a scenari in cui la verifica dell'identità del cittadino è sempre più spesso governata da terze parti non autorizzate; si pensi ad account gestiti da aziende private come Facebook e Google, per propri usi e per conto di terzi nell'ambito di schemi di autenticazione come OAuth 2.0. L'integrazione dei sistemi di Self Sovereign Identity con la tecnologia dei Distributed Ledger può condurre alla realizzazione su larga scala di questo nuovo paradigma.
- *Sviluppo di tecniche di anonimizzazione dei dati.* La garanzia della privacy di un utente non può essere ottenuta semplicemente offuscando l'identità del possessore di un certo dato, in quanto tale identità può essere inferita da altre informazioni relative al contesto nel quale il dato è stato prodotto/scambiato. Un importante obiettivo è la messa a punto di tecniche che consentano l'effettiva anonimizzazione dei dati rendendo impossibile la re-identificazione dell'utente.
- *Soluzioni centrate sull'utente per la protezione della privacy*. I cittadini debbono avere un ruolo attivo nella protezione dei propri dati, invece di quello passivo di oggi che permette solo di accettare o rifiutare le buone pratiche di protezione offerte da chi detiene i dati. Per questo servono soluzioni che consentano agli utenti di specificare preferenze di privacy e di stabilire quale informazione personale può essere rilasciata in dipendenza, ad esempio, della sensibilità dell'informazione, del ricevente, o del contesto applicativo.
- *Definizione di metriche di privacy e di utility*. La decisione di utilizzare una tecnica di protezione piuttosto che un'altra può dipendere dal trade-off tra la protezione offerta e le funzionalità garantite. Per questo è necessario definire delle metriche che consentano agli utenti di valutare i rischi di privacy a cui i dati sono esposti e l'utilità dei dati protetti in termini di capacità di supportare elaborazioni e di possibili errori introdotti nelle elaborazioni.
- *Sviluppo di piattaforme di data market*. Queste piattaforme debbono consentire la commercializzazione anche di dati privati ma in modo sicuro e controllato, nel pieno rispetto delle normative e delle esigenze dei diversi soggetti coinvolti, nonché la ricerca di informazioni e il loro acquisto, con la garanzia dell'integrità e correttezza dei dati ottenuti.

Impatti

Le linee di ricerca elencate in questa articolazione sono rilevanti in quanto possono cambiare alcuni aspetti fondamentali dell'interazione tra imprese, tra cittadini e imprese, tra cittadini e P.A., oltre che migliorare l'interazione tra i cittadini stessi. In particolare, si prevedono i seguenti impatti:

- La definizione di sistemi di tracciamento comporterà l'aumento della trasparenza di filiere e, in particolare, consentirà la certificazione dei prodotti del "Made in Italy", aumentando la consapevolezza dei consumatori nei confronti di prodotti di marchio italiano.
- La definizione delle metodologie e delle tecniche descritte porterà a un miglioramento del rapporto del cittadino con la pubblica amministrazione e quindi ad un incremento del livello di fiducia del cittadino nei confronti delle istituzioni.

- La definizione di strumenti per la verifica delle fonti supporterà il cittadino nella verifica delle informazioni reperite attraverso i social media e, in generale, attraverso la rete.
- La definizione di tecniche per permettere ai cittadini di mantenere il controllo su chi e come può usare i loro dati consentirà loro di aver maggior fiducia nelle infrastrutture digitali che usano nuove tecnologie e la garanzia che i loro dati siano adeguatamente protetti.
- La definizione di tecniche sofisticate di protezione e di anonimizzazione dei dati consentirà un uso dei dati mirato a difendere contemporaneamente l'interesse del singolo cittadino e quello dell'intera collettività.

Key Performance Indicators

- Quantità ed efficacia dei Distributed Ledger sviluppati
- Quantità di certificazioni di filiere industriali
- Quantità di processi tracciati mediante Distributed Ledger Technology
- Sensibilizzazione dei cittadini al problema della affidabilità delle fonti e della privacy dei dati
- Numero di strumenti sviluppati per la verifica dell'affidabilità delle fonti
- Numero di strumenti sviluppati per garantire al cittadino opportuni livelli di privacy
- Pubblicazioni ad alto impatto nella comunità scientifica e attività imprenditoriali nel settore (spin-off, startup).

Articolazione 5. Ecosistema della cybersecurity

La cybersecurity è parte di un sistema complesso, dinamico e multicomponente, fondato su una visione orientata ai processi di gestione, certificazione, assessment, standardizzazione e *compliance* della sicurezza. Le linee di azione, caratterizzate da componenti interdisciplinari, hanno lo scopo di inquadrare aspetti tecnologici e metodologici anche formali per il governo dei processi di sicurezza, tipicamente basati sulla *gestione del rischio*, per tutto il ciclo di vita di processi, servizi e prodotti. Di importanza basilare è il principio più volte menzionato della *security by design*, non solo nello specifico dominio dell'ingegneria del software, ma più in generale nell'intero processo di gestione dei progetti IT, declinato anche attraverso approcci formali e simulativi, quali *formal verification* e *metodologie di testing*, anche al fine di supportare e migliorare i processi di *cybersecurity certification* e *accreditation* di prodotti e processi. Un tema di ricerca di elevato valore strategico, anch'esso legato ai processi di *certification, assessment* e *compliance*, riguarda la *governance* della cybersecurity per migliorare la capacità delle organizzazioni complesse di adottare strategie di mitigazione del rischio attraverso modelli sempre più accurati di *risk quantification*, e modelli decisionali a supporto della sua corretta gestione (*risk management*). L'approccio risk-based è solo una delle prospettive dalle quali è possibile identificare la stretta relazione che le problematiche di cybersecurity hanno rispetto a diversi ambiti disciplinari, primo fra tutti quello dell'economia, attraverso i quali è possibile identificare i meccanismi che regolano l'equilibrio e l'efficacia dell'ecosistema della sicurezza.

La ricerca deve porsi come obiettivo generale l'innalzamento delle conoscenze scientifiche e tecnologiche utili al consolidamento di una visione della cybersecurity che combini opportunamente metodologie, processi, tecnologie, aspetti economico-gestionali, al fine di ottenere modelli di gestione, controllo e valutazione della sicurezza.

Nel resto seguito vengono descritti obiettivi di ricerca afferenti ad ambiti di diverso tipo, che vanno dalla definizione di standard per la governance della cybersecurity in organizzazioni complesse, alla gestione del rischio, alle metodologie che attribuiscono alla sicurezza e alla privacy un ruolo rilevante nelle strategie di progettazione IT, al tema della certificazione in ambito cybersecurity.

A. **Standard, best practice e certificazioni cyber**
B. **Analisi e di gestione del rischio cyber**
C. **Security e privacy by design**

Obiettivi

A. Standard, best practice e certificazioni cyber

La realizzazione di un ecosistema della sicurezza che, in accordo all'evoluzione normativa sovranazionale indotta dalla NIS, richiede di adottare la visione di un mercato unico digitale europeo che assicuri un livello elevato di sicurezza delle reti e dei sistemi informativi in maniera uniforme per tutti gli stati membri, evidenzia il ruolo strategico che hanno gli standard e le certificazioni. Occorre quindi che la comunità scientifica del settore riservi attenzione a questi aspetti, per garantire un costante sforzo al fine di essere al passo con l'evoluzione delle tecnologie, delle norme, e con l'incremento della complessità che la pervasività dei sistemi IT in ogni comparto della società ha determinato. Relativamente alle certificazioni, è importante citare il D.L. 105/2019, denominato *perimetro di sicurezza cibernetica*. Tale decreto ha come obiettivo principale quello di definire l'insieme delle misure che saranno adottate per richiedere elevati livelli di sicurezza delle reti dei sistemi informativi e dei sistemi informatici. Il livello di sicurezza richiesto dovrà essere garantito durante l'espletamento dei servizi offerti, evitando che malfunzionamenti o interruzioni possano impattare negativamente sull'intera sicurezza nazionale. Il decreto contempla l'attivazione del *CVCN (Centro di Valutazione e Certificazione Nazionale)* che ha l'onere di contribuire alla redazione delle misure di sicurezza e viene chiamato a valutare, nel caso di acquisti di tecnologie estere di beni e servizi ICT, l'opportunità di effettuare test su software o hardware. Il CVCN, inoltre, può elaborare e adottare adeguati schemi di certificazione. In questo quadro, è possibile identificare i seguenti obiettivi:

- *Incrementare il grado di maturità degli standard e delle best practices*. Tale obiettivo consiste della definizione di nuovi standard (e best practice) o nel miglioramento di quelli esistenti sia relativi ad ambiti di azione consolidati (come, ad esempio, gestione della sicurezza in organizzazioni complesse, *incident response, digital forensic, security operation center, risk assessment, cloud security*, etc.) sia in riferimento a nuovi scenari, come ad esempio *blockchain forensics*, gestione della sicurezza in ambito veicolare, sicurezza e affidabilità di sistemi basati su intelligenza artificiale e su smart contract, assessment di sicurezza di *smart grid*, cybersecurity per Industria 4.0, gli ambiti del dominio *health-care*, ancora non sufficientemente coperti.
- *Acquisire maggiore capacità di verifica della compliance*. Tale obiettivo si riferisce alla ricerca di metodologie e di strumenti, il più possibile automatizzabili, per il supporto all'applicazione di standard di sicurezza e per la verifica (misurabile) del grado di compliance agli stessi.
- *Incrementare la visione cognitiva del complesso di standard di cybersecurity*. Considerato che il gli standard di cybersecurity sono innumerevoli e tenuto conto delle implicazioni che l'applicazione congiunta degli standard può determinare, occorre migliorare la visione complessiva dell'intero sistema normativo sugli standard di cybersecurity, anche avvalendosi di approcci basati sul "normative reasoning". Ad esempio, per applicazioni safety-critical (e.g., avionico, ferroviario, difesa) e per quelle security-critical, è necessario considerare le relazioni e le eventuali dipendenze tra gli standard di dominio. Infatti, per un dato prodotto è possibile che sia richiesta, oltre alla certificazione di sicurezza, anche una certificazione di safety o viceversa. Diventa quindi importante effettuare studi per l'analisi congiunta e comparata di aspetti di sicurezza e di safety (e.g., valutare se un meccanismo di safety aumenti la vulnerabilità ad attacchi di sicurezza). Inoltre, è necessario studiare strategie di certificazione rispetto sia alla safety sia alla security, attraverso il riuso delle evidenze di certificazione tra più standard.
- *Certificazioni di prodotto.* Diversi standard richiedono l'adozione di un processo di sviluppo rigoroso e l'applicazione di best practice, ma la certificazione di processo fornisce solo indirettamente una garanzia della sicurezza del prodotto finale, e non sempre tiene in considerazione metodi di security planning e analisi del rischio. È pertanto desiderabile ottenere prove concrete delle proprietà di sicurezza attraverso la certificazione di prodotto e sviluppare soluzioni che dimostrino la sicurezza del prodotto messo in esercizio, attraverso procedure di attacco e l'analisi di metriche di prodotto.
- *Integrazione di sistemi COTS*. Nei prodotti complessi è necessario far coesistere componenti certificate con COTS (Component-Off-The-Shelf), quali prodotti software commerciali, sistemi operativi, progetti open-source, schede hardware, ..., che di norma non lo sono. Per chi utilizza un prodotto certificato è di fondamentale capire come integrarlo con componenti non certificate. In questo scenario, l'integratore non può sempre disporre di know-how sul funzionamento interno del componente stesso. Infatti, in alcuni casi i

COTS non sono accompagnati dal codice sorgente o da altri artefatti di progettazione generati durante il ciclo di sviluppo. È quindi necessario sviluppare soluzioni ad-hoc per la valutazione della sicurezza di COTS utilizzando ad esempio tecniche di analisi statica e dinamica dei programmi.

B. Analisi e di gestione del rischio cyber

Anche se il risk assessment è parte integrante di ogni metodologia che si ponga l'obiettivo di gestire la sicurezza nelle organizzazioni, il tema della gestione del rischio ha uno spessore tale da determinare specifici obiettivi di ricerca ad elevato interesse.

- *Migliorare i modelli e le metodologie di risk quantification*. Uno degli obiettivi prioritari da perseguire nel campo dell'analisi e gestione del rischio è la definizione di modelli e metodologie per la quantificazione del rischio. Sebbene esistono diversi approcci, anche largamente utilizzati in contesti aziendali, permane l'esigenza di migliorare l'accuratezza delle tecniche di quantificazione del rischio, che sono alla base di una corretta gestione del rischio stesso. Tale obiettivo può essere raggiunto delimitando il campo d'azione a specifici settori di interesse (ad es, finanziario, IoT, energia) o orientando l'analisi verso lo specifico settore della cyber *insurance* e avvalendosi di approcci quantitativi innovativi, come ad esempio le tecniche di simulazione. Questo obiettivo di ricerca ha forti connotati interdisciplinari, intersecandosi in maniera significativa con gli ambiti dell'economia e dell'organizzazione aziendale.
- *Realizzazione di strumenti di supporto alla gestione del rischio.* A questo obiettivo possono corrispondere diverse direzioni da seguire. Alcune linee di ricerca considerano gli aspetti semantici alla base di un trattamento automatico del problema, partendo dall'esigenza di far evolvere i modelli ontologici utilizzati in ambito di risk management e risk quantification (si consideri ad esempio il framework FAIR). Altre linee di ricerca considerano approcci basati su formalismi logici e rappresentazione del ragionamento probabilistico (o di altre tipologie di approcci utilizzabili per trattare l'incertezza nel ragionamento) o approcci *model-based,* al fine di automatizzare e migliorare il processo di assessment e di controllo del rischio. Altre ancora mirano a migliorare il supporto automatico alla gestione del rischio attraverso approcci di business intelligence e machine learning.

C. Security e privacy by design

Il ciclo di vita dei moderni sistemi software richiede di considerare gli aspetti legati alla sicurezza già dalle fasi di analisi e fino alla verifica del sistema stesso. I progressi della ricerca scientifica, accomunati nell'espressione security-by-design, hanno messo a disposizione degli sviluppatori diversi strumenti che si applicano, prevalentemente, alle fasi di sviluppo, di progettazione e di testing. Inoltre, il Regolamento 679/2016 ("GDPR") ha disposto nella pratica l'estensione del concetto di security-by-design anche alle misure di protezione della privacy. L'articolo 25 del GDPR, ad esempio, definisce che sia al momento di determinare i mezzi del trattamento (fase di design delle soluzioni) sia all'atto del trattamento stesso (fase di realizzazione), il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire la conformità della soluzione disegnata ai principi e le tutele fondamentali previste, garantendo che siano trattati esclusivamente i dati personali necessari per ogni specifica finalità del trattamento. Nonostante le linee guida e le tecniche esistenti, molti sistemi software presentano diverse vulnerabilità che permettono ancora di sferrare con successo diversi attacchi. L'obiettivo specifico è quindi quello di migliorare e rendere più efficienti gli strumenti atti a supportare l'incremento di qualità del codice, estendendo la loro adozione all'intero ciclo di sviluppo. In questo quadro, è possibile individuare i seguenti obiettivi:

- *Model-driven design.* Un caso interessante di tecniche che, fino a qualche anno fa erano note prevalentemente nella comunità scientifica, è rappresentato dai linguaggi per la specifica delle proprietà del software. Questi linguaggi permettono di comparare (semi-)automaticamente le proprietà formalizzate in fase di specifica con il codice sviluppato nelle fasi successive e con il sistema risultante. Ciò permette di riconoscere le falle di sicurezza che derivano da implementazioni che non rispettano la specifica. Più in generale, l'obiettivo di migliorare gli approcci e le tecniche di model-driven design può apportare differenti vantaggi. Le due direzioni di ricerca da investigare riguardano i due principali fondamenti del model-driven design, ovvero l'evoluzione dei linguaggi di modellazione specifici di dominio e la definizione di motori di

trasformazione e generazione automatica. Nella prima direzione rientrano lo sviluppo di nuovi linguaggi, efficaci nella formalizzazione della specifica, e l'estensione di linguaggi di modellazione esistenti per tenere meglio in conto i requisiti di sicurezza e di privacy dei sistemi software. Nella seconda direzione, invece, rientrano lo sviluppo di trasformazioni e di tecniche di composizione di trasformazioni per supportare la generazione sia di codice sia di artefatti di supporto durante l'intero ciclo di sviluppo.

- *Testing.* La verifica della sicurezza e della privacy di un prodotto software passa sicuramente per il testing del sistema stesso. L'obiettivo di testare per scoprire le vulnerabilità del sistema e determinare che i suoi dati e risorse siano protetti da possibili intrusioni, offre diverse direzioni di ricerca in linea con le focus area che vengono considerate solitamente nelle applicazioni web, ovvero network security, system software security, server-side application security e client-side application security. In ciascuna di esse, vanno considerati diversi aspetti, quali la generazione automatica dei casi di test, la loro riduzione, l'esecuzione automatica, la verifica automatica degli esiti e della copertura. Il fine ultimo di questo obiettivo di ricerca è rendere maggiormente efficace il testing al fine di verificare la security e la privacy dei sistemi software, garantendone la compliance rispetto agli standard e alle normative, oltre che rispetto ai requisiti specifici.
- *Formal verification.* L'adozione di metodi formali nelle diverse aree riguardanti lo sviluppo software, la verifica dell'hardware e dei sistemi embedded, migliora notevolmente la qualità dei prodotti sviluppati. I metodi formali possono offrire miglioramenti anche agli aspetti di sicurezza e di privacy in quanto possono offrire verifiche relative agli obiettivi di security in sistemi distribuiti, con diversi componenti interagenti. Essi possono anche essere un mezzo per controllare che un artefatto non offra punti di entrata agli attaccanti. Le direzioni di ricerca in questo campo sono dunque molteplici e riguardano sia lo sviluppo di nuove tecniche che tengano conto di aspetti legati alla scalabilità della verifica di proprietà formali, sia lo sviluppo di approcci che consentano la riduzione del gap tra il sistema modellato ed il sistema reale, che rappresenta la principale lacuna dell'adozione dei metodi formali. L'incremento stesso dell'usabilità dei metodi formali in realtà aziendali rappresenta una direzione di ricerca e innovazione.

Impatti

- Il raggiungimento degli obiettivi di ricerca di questa articolazione comporterà benefici ai fini del raggiungimento delle finalità previste dal D.L. sul perimetro nazionale.
- L'innovazione nell'ambito degli standard relativi a un certo dominio determina benefici economici per il segmento di mercato correlato al dominio stesso, con risparmio di risorse finanziarie nella misura in cui siano disponibili strumenti automatici a supporto dell'adozione degli standard e della verifica di compliance.
- Il consolidamento degli approcci di progettazione basati sul principio della security-by-design comporterà benefici in termini di qualità dei prodotti IT, e, di conseguenza, un migliore posizionamento dei prodotti nel mercato non solo nazionale.
- La realizzazione di modelli e metodologie per la gestione del rischio più precise determinerà vantaggi in termini di capacità delle organizzazioni di mitigare il rischio cyber in maniera efficace ed efficiente e darà un impulso significativo allo sviluppo del segmento dell'insurance in ambito cybersecurity.
- Il raggiungimento degli obiettivi di ricerca relativi alla certificazione determinerà benefici per l'industria IT, grazie all'identificazione di nuovi segmenti di mercato e al supporto fornito ai processi di certificazione anche in ambito di *system integration*.

Key Performance Indicators

- Sviluppo di sistemi o linguaggi che implementano i metodi proposti, messi a disposizione della comunità scientifica.
- Composizione di adeguati dataset per le sperimentazioni e diffusione della cultura sperimentale nella comunità, con condivisione dei dataset, dei package e delle repliche sperimentali.
- Numero di nuovi framework, best practice, (draft) standard prodotti in ambito cybersecurity.

- Numero di tool per l'assessment per la compliance con standard e per il supporto alla gestione del rischio.
- Acquisizione di maggiore capacità di integrare in maniera interdisciplinare le diverse componenti (informatica, economico-aziendale, legale) dell'ecosistema della cybersecurity nel dominio della ricerca e in quello del trasferimento dei risultati nel contesto produttivo.
- Sensibilizzazione delle aziende di IT nei riguardi del principio della *security and privacy by design*, con progressiva trasformazione dei processi di progetto, anche in termini di formazione dei team e di interazione tra le diverse business unit dell'azienda.
- Promozione e diffusione della certificazione delle organizzazioni (private e pubbliche) in ambito di governance e organizzazione della cybersecurity e della visione risk-based su cui esse si fondano.
- Pubblicazioni ad alto impatto nella comunità scientifica e attività imprenditoriali nel settore (spin-off, startup).

Articolazione 6. Infrastrutture di ricerca per la cybersecurity

Per difendersi dagli attacchi cyber, perpetrati da organizzazioni criminali sempre più strutturate e articolate, ma anche da attori collegati a stati sovrani, è necessario mettere a punto una politica nazionale di cybersecurity che, in un settore in così rapida evoluzione, metta al centro la ricerca. Solo un approccio guidato dalla ricerca potrà fornire la garanzia della disponibilità di una conoscenza approfondita delle sempre nuove vulnerabilità a tutti i livelli, delle metodologie di attacco e di difesa, e potrà quindi dare la possibilità di organizzare al meglio le difese. Un ecosistema di cybersecurity coordinato permetterà di sviluppare anche nel nostro Paese metodologie e strumenti di avanguardia che metteranno in grado le nostre aziende cyber di competere nel mercato internazionale, creando un contesto stimolante che inviterà i giovani talenti cyber italiani a rimanere o rientrare nel nostro Paese. Un passo importante verso lo sviluppo dell'ecosistema cyber nazionale è stata l'istituzione del cosiddetto "Perimetro di sicurezza nazionale cibernetica" (Legge 18 novembre 2019, n. 133), che definisce un'area di protezione rafforzata degli asset ICT strategici, in un quadro di forte sinergia inter-istituzionale e pubblico-privato e che, in un contesto di mancanza di autonomia tecnologica del mercato digitale italiano ed europeo, prevede meccanismi di test per individuare vulnerabilità di sicurezza dei prodotti e per verificare l'affidabilità dei soggetti che intendono offrire beni e servizi ICT destinati a essere impiegati in reti e sistemi che svolgono funzioni essenziali per il Paese.

Perché quanto sopra delineato diventi fattibile è necessario operare in modo coordinato tra privato e pubblico, militare e civile. Il DPCM del febbraio 2017 in materia di sicurezza cibernetica[8] fornisce il riferimento nazionale strategico e operativo entro cui operare e pone le basi per un ventaglio articolato di azioni, iniziative e centri all'avanguardia, quali il *Nucleo di Sicurezza Cibernetica* (NSC), il *Centro Nazionale di Ricerca e Sviluppo in Cybersecurity*, il *Laboratorio Nazionale di Crittografia*, il *Cyber Range Nazionale* e il *Centro di Valutazione e Certificazione Nazionale* (CVCN), il *Computer Security Incident Response Team (CSIRT)* italiano. Alcuni di queste iniziative, quali l'NSC, il CVCN e lo CSIRT, sono già state finalizzate. Altre, sebbene necessarie per supportare una *politica nazionale cyber,* sono invece ancora da realizzare. Si ritiene importante partire al più presto con azioni concrete che mettano a disposizione, in programmi pluriennali, le risorse necessarie per creare quelle infrastrutture di ricerca che altri paesi europei hanno già avviato da tempo.

Nel resto di questa scheda si forniranno alcune indicazioni sul tipo di infrastrutture che sono necessarie per fornire il supporto alla ricerca in cybersecurity e lo sviluppo di strumenti adeguati alla prevenzione degli attacchi e per incrementare la resilienza del sistema Paese. In particolare, indicheremo come obiettivi la creazione delle seguenti infrastrutture:

A. **Rete Nazionale di Laboratori di Ricerca in Cybersecurity**
B. **Reti di Addestramento e Osservatori di Rete**
C. **Blockchain Nazionale**

[8] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf

D. Rete di Centri per Servizi Sicuri

Queste infrastrutture dovrebbero essere definite quanto prima e supportate per tutta la durata del Piano Nazionale.

Obiettivi

A. Rete Nazionale di Laboratori di Ricerca in Cybersecurity

La struttura portante di questo ecosistema è costituita da una rete di centri di competenza costruita attorno a un *Centro Nazionale di Ricerca in Cybersecurity* e che prevede *Centri Territoriali* e *Centri Verticali*.

Il *Centro Nazionale di Ricerca in Cybersecurity* dovrà attrarre ricercatori e investitori pubblici e privati (nazionali) e rappresentare il collante tra università e centri di ricerca italiani, il settore produttivo e il settore governativo, per contribuire alla definizione e al raggiungimento degli obiettivi strategici nel settore. Il centro concorrerà anche a creare competenze di alto profilo, a generare spin-off di settore, a sviluppare la ricerca e a definire metodologie e strumenti a supporto delle certificazioni nazionali, fornendo il necessario supporto tecnologico ai costituendi laboratori accreditati dal CVCN (Centro di Valutazione e Certificazione Nazionale). Il Centro dovrà operare in stretta sinergia con il mondo universitario e della ricerca scientifica, cooperando con i centri di eccellenza sparsi sul territorio nazionale. Il Centro potrà anche erogare servizi ad alto contenuto innovativo verso le organizzazioni governative, la PA, le forze di polizia e gli apparati investigativi e dovrà operare in stretta sinergia con i centri omologhi presenti in Inghilterra, Francia, Germania e Stati Uniti, ricoprendo anche, verso l'Europa, il ruolo di Centro di Eccellenza Nazionale all'interno dei programmi comunitari di cybersecurity, in modo da essere il riferimento nazionale per il nascituro Centro Europeo di competenza industriale, tecnologica e di ricerca sulla cybersecurity.

All'interno del Centro potrebbe trovare adeguata collocazione anche il *Laboratorio Nazionale di Crittografia* per coniugare al meglio teoria e pratica, mettendo a fattor comune le tante conoscenze matematiche della nostra accademia e la lunga tradizione dei nostri apparati militari nel settore della crittografia.

I Centri Territoriali di Competenza in Cybersecurity dovranno essere distribuiti in ambiti territoriali con valenza di città metropolitana, regionale o interregionale, basandosi su una stretta collaborazione a livello locale tra il sistema universitario, gli enti pubblici di ricerca, le imprese private e la pubblica amministrazione locale. Questi centri si occuperanno di innovazione in ambito cyber, curando il trasferimento tecnologico, la formazione, la consulenza e il supporto alle aziende, alle pubbliche amministrazioni, ai professionisti e ai cittadini di quel territorio.

I Centri Verticali di Competenza in Cybersecurity dovranno rispondere alla necessità di settori di mercato specifici, quali, ad esempio, energia, trasporti, sanità, finanza. I vari attori potranno utilizzare i centri verticali, da un lato, per rispondere alla necessità di disporre di centri in grado di sviluppare attività di cybersecurity dedicate allo specifico dominio e, dall'altro, per garantire la condivisione delle informazioni, attraverso tavoli di scambio e di analisi, nella consapevolezza che la condivisione delle informazioni su possibili o effettivi attacchi è alla base di qualunque strategia di difesa cyber.

B. Reti di Addestramento e Osservatori di Rete

Per aumentare le capacità di difesa di aziende e pubbliche amministrazioni sia centrali sia periferiche, e per mettere in grado i ricercatori di costruire strumenti di *early warning* e competere a livello internazionale, è necessario sviluppare specifiche infrastrutture di ricerca quali una rete di *Cyber Range*[9] per la formazione e l'addestramento "sul

[9] I *Cyber Range* sono poligoni virtuali dedicati all'addestramento sia dei professionisti del settore sia dei giovani ricercatori. Sono costituiti da ambienti e sistemi controllati, tipicamente basati sulla virtualizzazione, che si prestano a un'ampia varietà di impieghi quali la formazione e l'aggiornamento individuale alla cybersecurity tramite lo svolgimento di esercizi pratici; l'addestramento e valutazione delle capacità di squadre di operatori mediante lo svolgimento di esercitazioni; la progettazione, sviluppo e testing di nuove tattiche, tecniche e procedure di cybersecurity; la valutazione delle capacità di difesa di un sistema.

campo" e una rete di *Honeypot*[10] intelligenti che possa essere utilizzata per costruire una banca dati nazionale delle minacce e per fornire ai ricercatori gli strumenti necessari per individuare tempestivamente i possibili vettori di attacco. Alla rete di honeypot potranno essere affiancati anche dei cosiddetti "telescopi di rete" ovvero sistemi che consentono di monitorare eventi su larga scala che si svolgono su Internet osservando il traffico indesiderato di ritorno (*backscattering*) tipicamente dovuto all'attività di attacchi o di diffusione di malware di vario genere.

Una rete nazionale di cyber range che integri quanto già disponibile in ambito privato, pubblico, militare e governativo, e che possa eventualmente coinvolgere anche cyber range europei e cyber range specializzati su diversi settori (IoT, Infrastrutture Critiche, Servizi di PA, droni, ...) permetterebbe di sperimentare sul campo avanzate tecniche di difesa ad ampio spettro e a migliorare la resilienza.

Una rete di honeypot nazionale è funzionale alla minimizzazione del tempo di scoperta dell'attacco, alla protezione di dati e applicativi, alla creazione di una banca nazionale delle minacce che sia in grado di garantire autonomia nel riconoscimento di malware e supporto all'analisi forense e alla gestione delle prove. La rete di telescopi permette invece di ottenere informazioni utili per alimentare modelli di individuazione e previsione di attacchi.

C. Blockchain Nazionale

La tecnologia dei registri distribuiti (distributed ledger), progettata per resistere alla modifica fraudolenta dei dati, è attualmente considerata una reale alternativa, in termini di sicurezza, affidabilità, trasparenza e costi, ai registri gestiti in maniera centralizzata da autorità riconosciute e regolamentate (pubbliche amministrazioni, banche, assicurazioni, intermediari di pagamento, ecc.). Per questo l'uso di registri distribuiti può portare significativi miglioramenti alla gestione dei diritti digitali, alla protezione di brevetti e marchi, alle catene di fornitura globali, alle transazioni finanziarie, alla fornitura di servizi della pubblica amministrazione. I registri di atti notarili, i registri di imprese, il catasto e i protocolli sono ottimi esempi di applicazioni che potrebbero beneficiare di una blockchain. La disponibilità di una blockchain nazionale sarebbe importante per i ricercatori per sperimentare nuovi servizi che necessitano di un controllo normativo e di elevate garanzie in termini di integrità e di verifica di dati e funzioni. Una blockchain nazionale sarebbe anche un utile strumento per la ricerca e la definizione di strumenti per il rilevamento di transazioni e di comportamenti illegali e per la sperimentazione degli *smart-contract* che vengono utilizzati per prendere decisioni automatiche in base a schemi predeterminati che tengono conto di sopraggiunte informazioni o variate condizioni al contorno. La blockchain nazionale potrà anche essere un'ottima base per la ricerca sul mercato delle criptovalute. L'importanza dell'uso di blockchain è stata recentemente anche sottolineata dal gruppo di esperti MISE che ha elaborato un documento[11] sulla strategia italiana su blockchain dove vengono dettagliati innumerevoli possibili usi di questa tecnologia.

D. Rete per Servizi Sicuri

Per supportare adeguatamente la ricerca e garantire la riservatezza dei risultati in alcune aree strategiche è opportuno mettere a disposizione della comunità scientifica un insieme di infrastrutture nazionali sicure per la memorizzazione, il calcolo, la certificazione e la comunicazione. Tali infrastrutture potrebbero essere realizzate a partire da quelle che già attualmente sono gestite da consorzi interuniversitari quali il GARR[12], che gestisce la banda ultralarga, e il CINECA[13], che fornisce vari servizi applicativi e di calcolo.

Un obiettivo primario da perseguire attraverso una forte collaborazione tra CINECA e GARR dovrebbe essere quello di offrire a tutti ricercatori strumenti interoperanti di elaborazione, di comunicazione, di video conferenza e memorizzazione di grosse quantità di dati, garantendo efficienza, facilità d'uso, privacy e soprattutto piena

[10] Le *honey pot* si presentano come parte di un sito web con dati o risorse di interesse per eventuali attaccanti, ma, nei fatti, fanno parte di un sito isolato e monitorato che viene usato come "esca" per studiare le intenzioni o le strategie di eventuali attaccanti.
[11] https://www.mise.gov.it/images/stories/documenti/Proposte_registri_condivisi_e_Blockchain_-_Sintesi_per_consultazione_pubblica.pdf
[12] https://www.garr.it
[13] https://www.cineca.it

confidenzialità dei dati scientifici. I consorzi di cui sopra potrebbero fornire congiuntamente il supporto per l'attivazione e la realizzazione di tutte le reti di honeypot per malware e di telescopi di rete e per la blockchain nazionale, nonché fornire supporto alla rete dei laboratori di ricerca in cybersecurity.

Da un punto di vista più generale, i due consorzi, in collaborazione, potrebbero supportare un'ampia sperimentazione relativa alla digitalizzazione dei servizi che, garantendo l'utilizzo di strumenti digitali per la dematerializzazione di documenti e per lo scambio, la certificazione e la conservazione dei dati, accompagni la transizione digitale del nostro Paese. La sperimentazione potrebbe partire proprio dal ricettivo settore della ricerca per poter poi essere estesa a tutta la Pubblica Amministrazione. Uno degli obiettivi dovrebbe essere quello di creare le condizioni affinché tutti i dati, gli scambi, le informazioni relative a cittadini italiani siano nella grande maggioranza dei casi memorizzati su server nazionali o almeno europei. Al momento, purtroppo, la maggior parte dei servizi di memorizzazione, comunicazione, video conferenza ed elaborazione sono forniti da società extra europee che fanno profitti non solo sulla vendita di tali servizi ma anche sulla commercializzazione dei dati dei loro utenti.

Impatti

Aumentare la resilienza del sistema Paese, delle aziende e della PA, relativamente agli attacchi cyber attraverso un insieme di strutture che, coordinandosi, alzino il livello della protezione cibernetica del Paese e siano collegati agli *innovation hub* europei, candidando l'Italia a giocare un ruolo chiave come Centro Europeo di Cybersecurity. La collaborazione tra le diverse strutture sarà un fattore chiave di successo, in quanto permetterà non solo di ridurre i costi del processo di innovazione, ma anche di estendere la portata di progetti innovativi, sfruttando le complementarietà delle realtà coinvolte, attraverso opportune sinergie. Disporre di informazioni tempestive, complete e affidabili permette decisioni più consapevoli e accelera le azioni di protezione durante la normale operatività, come pure le azioni di rilevamento, reazione, contenimento e ripristino in tempo di crisi.

La rete di cyber range è funzionale a mettere a fattor comune dei poligoni virtuali dedicati all'addestramento dei professionisti del settore, costituiti da ambienti e sistemi controllati che si prestano a un'ampia varietà di impieghi, quali la formazione e l'aggiornamento individuale alla cybersecurity, l'addestramento e la valutazione delle capacità di squadre di operatori mediante lo svolgimento di esercitazioni, la valutazione e la messa a punto di nuove tattiche e tecniche di difesa.

Una rete nazionale di honeypot e telescopi di rete funzionerebbe da un lato come un osservatorio "sismografico" per monitorare, prevedere e prevenire campagne di attacchi e dall'altro permetterebbe di costruire archivi e dataset comportamentali riguardanti i diversi tipi di malware. I dati raccolti verrebbero messi a disposizione anche del Computer Security Incident Response Team (CSIRT) Italiano per le attività di prevenzione e preparazione a eventuali situazioni di crisi. Dati sui malware e altri attacchi sono difatti indispensabili per i ricercatori per mettere a punto nuove tecniche di identificazione malware basate su Intelligenza Artificiale e per fronteggiare attacchi avversariali all'Intelligenza Artificiale.

Una blockchain nazionale accelererebbe la sperimentazione sulla transizione digitale dei servizi pubblici e garantirebbe il miglioramento di tali servizi in termini di affidabilità, sicurezza, trasparenza e accessibilità, nonché una riduzione dei costi rispetto ai metodi tradizionali di memorizzazione e di elaborazione delle informazioni.

Riuscire a mantenere sul territorio nazionale i dati degli utenti relativi ai servizi forniti e renderli utilizzabili, garantendo privacy, alla comunità di ricerca avrebbe anche il vantaggio di fornire importanti strumenti di ricerca e indicazioni per le scelte strategiche delle aziende nazionali.

Key Performance Indicators

- Iniziative imprenditoriali (spin-off, start-up) per nuovi servizi digitali sicuri
- Nuovi servizi sicuri per le università e gli EPR
- Rapporti delle strutture di ricerca pubbliche con Pubblica Amministrazione ed Aziende
- Livello di utilizzazione della tecnologia blockchain e della blockchain nazionale
- Pubblicazioni ad alto impatto nella comunità scientifica.

Interconnessioni con altri Ambiti Tematici

Come discusso nella parte introduttiva, le tecnologie e gli strumenti informatici vengono utilizzati pervasivamente in tutti i settori della nostra società, e pertanto la cybersecurity impatta su quasi tutti gli aspetti della vita sociale e quindi su quasi tutti gli ambiti tematici del PNR 2021-2027.

Sicuramente il sottoambito cybersecurity è collegato a tutti i sottoambiti

- Aerospazio (nostra articolazione 1, 2 e 3)
- High Performing Computing (nostre articolazioni 3, 4 e 6)
- Innovazione per l'industria Manifatturiera (nostre articolazioni 2 e 4)
- Intelligenza Artificiale (nostra articolazione 3)
- Robotica (nostra articolazione 2 e 3)
- Tecnologie Quantistiche (nostra articolazione 3)
- Transizione Digitale - I4.0 (nostre articolazioni 1, 2, 3, 4, 5 e 6)

dell'ambito *Informatica, Industria, Aerospazio.*

Gli aspetti di cybersecurity, quali quelli trattati da noi nelle articolazioni 2, 3 e 4, sono importanti per la privacy ma anche per problematiche di attacchi a dispositivi medici o a sensori e attuatori, per i sottoambiti:

- Tecnologie per la Salute e
- Temi generali

dell'ambito *Salute.*

La cybersecurity è anche importante per l'utilizzo delle tecnologie blockchain (sviluppate nelle nostre articolazioni 4 e 6) per la protezione dei prodotti nazionali e per la lotta alle fake news per i sottoambiti:

- Creatività, Design e Made in Italy (articolazione 5)

dell'ambito *Cultura Umanistica, Creatività, Trasformazioni Sociali, Società dell'inclusione.*

Inoltre, la cybersecurity e in particolare le tematiche di ricerca della nostra articolazione 2, sono rilevanti per il sottoambito:

- Mobilità Sostenibile (articolazione 5 - "Mobilità automatizzata, connessa e sicura")

dell'ambito *Clima, Energia, Mobilità Sostenibile.*

Posizionamento Europeo

587 tra professori e ricercatori dislocati in 57 importanti Università e Istituti di ricerca italiani collaborano su tematiche relative alla cybersecurity all'interno del Laboratorio Nazionale di Cybersecurity del consorzio interuniversitario CINI. Il Laboratorio, che collabora alla costruzione dell'ecosistema nazionale italiano della sicurezza informatica, anche attraverso la promozione di un continuo processo di aggregazione tra strutture di ricerca e formazione in un'ottica multidisciplinare e interdisciplinare, permette ai suoi membri un ottimo posizionamento a livello internazionale, collaborando attivamente con istituzioni comunitarie ed extracomunitarie quali ENISA (The European Union Agency for Cybersecurity - https://www.enisa.europa.eu), ECSO (European Cyber Security Organization - https://www.ecs-org.eu/); NIST (National Institute of Standards and Technology USA - https://www.nist.gov), ...

Gruppi di ricerca in cybersecurity sono coinvolti in moltissimi progetti europei e in particolare in tutti i progetti pilota dell'iniziativa EU che punta a definire le strategie comunitarie sulla cybersecurity nei prossimi dieci anni.

Inoltre, numerosi ricercatori del Laboratorio sono coinvolti in importanti progetti di Ricerca e Sviluppo con grandi Aziende Multinazionali, sono Chair di prestigiose conferenze internazionali del settore e sovente le hanno attratte in Italia, ed *editor in chief* di riviste scientifiche qualificate. Il grado di partecipazione di ricercatori italiani di cybersecurity negli Editorial Board di riviste internazionali prestigiose, Steering e Program Committee di conferenze del settore è considerevole.