ICONOCRAZIA

RIVISTA DI SCIENZE SOCIALI E FILOSOFIA POLITICA

SAGGIO

La Mobilità Sostenibile nelle *Smart city*: Prospettive, Sfide e Soluzioni

MARIA TERESA BALDASSARRE, VITA SANTA BARLETTA, GIUSEPPE PIRLO, MICHELE SCALERA

Università degli Studi di Bari Aldo Moro

Abstract

Le città di tutto il mondo affrontano sfide crescenti in termini di congestione del traffico, inquinamento atmosferico e cambiamenti climatici. La *smart mobility* è emersa come una risposta cruciale a queste sfide, e le *smart city* offrono un terreno fertile per l'innovazione in questo settore. Questo studio si propone di esaminare il ruolo della mobilità sostenibile nelle *smart city*, analizzando prospettive, sfide e soluzioni.

Parole chiave: *smart city*, mobilità sostenibile, *smart mobility*, sfide urbane

English version

Cities around the world face growing challenges in terms of traffic congestion, air pollution and climate change. *Smart mobility* has emerged as a crucial response to these challenges, and smart cities offer fertile ground for innovation in this area. This study aims to examine the role of sustainable mobility in smart cities, analysing perspectives, challenges and solutions.

Keywords: *smart city*, sustainable mobility, *smart mobility*, urban challenges

***Smart mobility* e *Smart city*: Definizioni e Concetti Chiave**

Smart city o città intelligente si riferisce all'ideale collettivo della città del futuro, e nello specifico ad un'area urbana in grado di creare sviluppo economico e alta qualità della vita attraverso l'uso della tecnologia integrata e l'ottimizzazione delle risorse.

Il concetto di *smart city* è stato introdotto per la prima volta nel 1990 per incorporare nella pianificazione urbana hardware e software avanzati basati sulle tecnologie dell'informazione e della comunicazione (ICT) (Al Sharif e Pokharel 2022).

Se ben progettate le *smart city* potenzialmente possono migliorare la qualità della vita dei cittadini, promuovere l'economia, facilitare il processo di risoluzione dei problemi di trasporto e di traffico attraverso una gestione adeguata, nonché incoraggiare un ambiente pulito e sostenibile e fornire un'interazione accessibile con le autorità governative competenti.

Le tecnologie ICT diventano, di conseguenza, l'infrastruttura hardware, software e telematica per attuare un insieme di strategie di pianificazione urbanistica volte all'ottimizzazione e all'innovazione dei servizi pubblici e per mettere in relazione le infrastrutture delle città con il capitale umano, intellettuale e sociale di chi le abita.

Aletà *et al.* (2017) definiscono la *smart mobility* come un aspetto che consiste nell'insieme di atti che incoraggiano il flusso del traffico, sia a piedi che in bicicletta, o tramite mezzi di trasporto federali o statali, tutti perseguendo l'obiettivo condiviso di minimizzare i costi economici, ambientali e di tempo. Allam e Newman (2018), invece, sostengono che la *smart mobility* enfatizza l'integrazione della tecnologia nelle infrastrutture urbane e, dunque, si concentra su come le persone, che interagiscono con l'ambiente urbano, possono farlo in modo illuminato e sostenibile.

Il ruolo della *smart mobility* nelle *smart city* sta diventando sempre più cruciale per affrontare le sfide legate alla congestione del traffico, all'inquinamento dell'aria e ai cambiamenti climatici, e per creare città più vivibili e sostenibili.

La mobilità sostenibile mira a ridurre le emissioni di gas serra e l'inquinamento dell'aria attraverso l'uso di veicoli a basse emissioni o elettrici, l'implementazione di reti di trasporto pubblico efficienti e la promozione di modalità di viaggio a emissioni zero come il ciclismo e la mobilità a piedi.

Ne consegue che riducendo la congestione del traffico e l'inquinamento, la *smart mobility* contribuisce a migliorare la qualità della vita dei cittadini, rendendo le città vivibili e accoglienti anche in presenza di presidi industriali a volte troppo invadenti.

Non è di poco conto pensare che le tecnologie sottese alle *smart city* contribuiscono all'efficienza energetica complessiva del sistema di trasporto, riducendo la dipendenza dai combustibili fossili.

Inoltre, la *smart mobility* può garantire che i servizi di trasporto siano accessibili a tutti, compresi anziani e persone con disabilità. Ciò contribuisce all'uguaglianza e all'inclusione sociale.
Da tutto ciò ne consegue una città con esigenze ridotte di parcheggi su strada, consentendo l'uso più efficiente dello spazio urbano per scopi come parchi o edifici. Il verde urbano, appunto, sarebbe il primo beneficiario di una politica che supporti a 360 gradi il concetto di *smart city*.
In tale contesto anche la raccolta e il riciclaggio dei rifiuti possono essere ottimizzati utilizzando sensori che monitorano i livelli di riempimento dei bidoni (Rahman *et al.* 2022; Uganya *et al.* 2022). Inoltre, le tecnologie abilitanti possono essere utilizzate per sviluppare sistemi di agricoltura urbana, come giardini verticali e coltivazioni idroponiche, per promuovere l'accesso ad un cibo sempre più sano.
Le prospettive, dunque, sono quelle di migliorare la salute dei cittadini con una ricaduta positiva e significativa anche nella spesa pubblica sanitaria e includono una maggiore adozione di veicoli elettrici e l'espansione dei servizi di car sharing e bike sharing; la progettazione ed implementazione di reti di trasporto pubblico efficienti e integrate, con orari e percorsi personalizzati basati su dati in tempo reale e la promozione della mobilità a piedi e in bicicletta, con la creazione di piste ciclabili e percorsi pedonali sicuri.
La transizione verso la mobilità sostenibile richiede investimenti significativi in veicoli e infrastrutture a basso impatto ambientale. È di tutta evidenza che la costruzione di stazioni di ricarica, piste ciclabili e percorsi pedonali sicuri è essenziale per sostenere la mobilità sostenibile.
Tali investimenti tendono ad aumentare in presenza di infrastrutture stradali obsolete non adatte alla mobilità sostenibile.
La pianificazione urbana integrata per le *smart city* dovrebbe prevedere incentivi fiscali per l'adozione di tecnologie smart, come, per esempio, per l'acquisto di veicoli elettrici e promuovere le infrastrutture di ricarica; inoltre, dovrebbe contemplare lo sviluppo urbano in modo integrato, considerando la mobilità sostenibile come un elemento centrale.

Le competenze necessarie

Un progetto di smart city richiede un *team* multidisciplinare con una vasta gamma di competenze per garantire il successo.
Gli esperti in urbanistica e pianificazione urbana sono fondamentali per progettare e sviluppare l'infrastruttura fisica della smart city, tenendo conto della sostenibilità, della mobilità e delle esigenze dei cittadini. Gli specialisti in sostenibilità possono contribuire a garantire che il progetto sia in linea con gli obiettivi di sviluppo sostenibile e che sia attento all'ambiente.

In un gruppo di lavoro di questo tipo non possono mancare i professionisti della gestione dei progetti al fine di coordinare le varie fasi del progetto, pianificare le risorse e garantire che tutto proceda secondo i tempi e i budget stabiliti.
Come si può notare, dunque, le competenze necessarie sono multidisciplinari ed a queste bisogna aggiungere quelle degli esperti legali per garantire la conformità normativa e che, dunque, devono far applicare le leggi e i regolamenti relativi alla *privacy* dei dati, alla sicurezza, all'edilizia e alla gestione delle infrastrutture e quelle degli esperti in economia e finanza al fine di gestire i *budget* del progetto, identificare fonti di finanziamento e valutare il ritorno sugli investimenti.
Così come sono indispensabili gli ingegneri elettrici ed elettronici che sviluppano e gestiscono l'infrastruttura elettrica necessaria per supportare tecnologie come veicoli elettrici e illuminazione intelligente.
L'innovazione possibile è talmente invasiva e positiva che richiede un piano, non certo a costo zero, di sensibilizzazione pubblica per educare i cittadini sull'importanza della mobilità sostenibile e sulle opzioni disponibili; cittadini, si badi bene, spesso restii all'adozione di tali tecnologie sostenibili e di nuove modalità di trasporto. È indispensabile la promozione di un piano, che può anche essere complesso, della mobilità sostenibile al fine di stimolare la collaborazione tra enti pubblici, aziende private e comunità locali. Per tal motivo, nel *team* multidisciplinare non possono mancare gli specialisti in comunicazione e marketing al fine di diffondere informazioni sulla *smart city*, coinvolgere i cittadini e promuovere i servizi e le iniziative.
Dulcis in fundo gli esperti ICT: sono necessari per progettare, implementare e gestire le infrastrutture di rete, le soluzioni di cloud computing, la connettività IoT e le applicazioni software. Gli specialisti in data science sono indispensabili per analizzare i dati raccolti da sensori e altre fonti per la creazione di un sistema che estragga informazioni e conoscenza a supporto delle decisioni strategiche. Gli sviluppatori di software sono indispensabili per creare le applicazioni e i servizi digitali cuore pulsante delle smart city così come non possono mancare gli esperti in cyber security per proteggere le infrastrutture da minacce cibernetiche.

Tecnologie abilitanti

Le tecnologie abilitanti delle smart city sono una serie di strumenti e sistemi innovativi che permettono alle città di diventare più efficienti, sostenibili e intelligenti. Queste tecnologie sono essenziali per la raccolta, l'analisi e l'utilizzo dei dati in modo da migliorare la qualità della vita dei cittadini, ottimizzare le risorse e affrontare sfide urbane complesse.
Queste tecnologie lavorano insieme per rendere le città più intelligenti, sostenibili ed efficienti. La loro adozione è fondamentale per affrontare le sfide urbane e migliorare la qualità della vita dei cittadini.
Le principali tecnologie abilitanti sono:

- L'*Internet of Things*, IoT, a differenza della Internet che conosciamo che collega le persone, collega principalmente, attraverso Internet, gli oggetti, consentendo la raccolta di dati in tempo reale da dispositivi come sensori ambientali, telecamere di sicurezza, misuratori intelligenti e semafori intelligenti (Allam e Newman 2018).

Dagli orologi che monitorano la pressione sanguigna ai frigoriferi che incentivano ad acquistare più latte, dalle catene di montaggio "gestite" da robot ai droni che consegnano i pacchi, l'IoT promette un profondo impatto sugli individui e sulla società; esso si basa su un sistema che installa sensori e dispositivi di elaborazione in oggetti di uso quotidiano (ad esempio frigoriferi) collegandoli in reti che raccolgono e utilizzano dati sulle loro prestazioni.

L'Internet delle cose è reso possibile dai progressi nella capacità di miniaturizzare i dispositivi di scansione e di fornire loro una potenza di elaborazione sufficiente per monitorare l'attività, analizzare l'utilizzo e fornire risultati su reti elettroniche (Olson 2016).

Questi dati possono essere utilizzati per monitorare l'ambiente urbano, migliorare la gestione del traffico, ottimizzare l'illuminazione pubblica e molto altro.

- Big Data e Analisi dei Dati: La capacità di raccogliere, archiviare e analizzare grandi quantità di dati è fondamentale per prendere decisioni basate su evidenze empiriche. L'analisi dei dati consente di identificare tendenze, risolvere problemi e pianificare lo sviluppo urbano in modo più efficiente (Batty 2013; Mayer-Schönberger e Cukier 2013).
- Sistemi di Trasporto Intelligenti (ITS): utilizzano tecnologie avanzate per migliorare la gestione del traffico e la sicurezza stradale. Ciò include semafori intelligenti che si adattano al traffico in tempo reale, sistemi di segnalazione avanzati e comunicazioni veicolo-veicolo/veicolo-infrastruttura (Zaheer *et al.* 2019).
- Reti 5G: offrono una connettività ultraveloce e a bassa latenza, che è fondamentale per supportare l'IoT, le applicazioni di realtà virtuale e aumentata, nonché l'interconnessione di dispositivi in tempo reale nelle smart city (Garcia *et al.* 2021).
- Blockchain: La blockchain può essere utilizzata per garantire la sicurezza e la trasparenza dei dati e delle transazioni, ad esempio nell'ambito dell'identità digitale, della gestione energetica o dei servizi finanziari nelle città (Yaga *et al.* 2018; Taylor *et al.* 2020).
- Energia Rinnovabile e Architetture Energetiche Intelligenti: Le città intelligenti spesso sfruttano fonti di energia rinnovabile, come pannelli solari e turbine eoliche, e utilizzano sistemi di gestione energetica avanzati per ottimizzare il consumo e la distribuzione dell'energia.
- Mobilità Sostenibile: La promozione di modalità di trasporto sostenibili, come veicoli elettrici, biciclette condivise, car sharing e trasporto pubblico

intelligente, contribuisce a ridurre l'inquinamento e la congestione del traffico Aletà *et al.* 2017).

- Sistemi di Sicurezza e Sorveglianza: Le tecnologie di sicurezza come telecamere di sorveglianza, riconoscimento facciale e sensori acustici aiutano a garantire la sicurezza pubblica e a prevenire il crimine (Yan *et al.* 2022; Smith e Miller 2022).
- Applicazioni mobile: Le applicazioni mobili e i portali online consentono ai cittadini di accedere a servizi pubblici, fornendo informazioni in tempo reale su traffico, trasporto pubblico, qualità dell'aria e molto altro.

Edifici e Case Intelligenti: Le tecnologie abilitanti consentono la gestione efficiente dell'energia e delle risorse in edifici intelligenti attraverso il controllo centralizzato dei sistemi di riscaldamento, raffreddamento, illuminazione e sicurezza (Umair *et al.* 2021; Mir *et al.* 2021).

Sicurezza informatica

La mobilità del futuro, secondo EY e IIA (EY and IIA 2021) sarà caratterizzata dalle seguenti tecnologie: Micro-mobilità tascabile per coprire spostamenti brevi con mezzi leggeri e meno inquinanti; *Drone-taxi*, veicoli aerei senza pilota adibiti al trasporto di passeggeri e supportati da sistemi di intelligenza artificiale; Veicoli completamente autonomi, equipaggiati da una serie di sensori come GPS, telecamere e/o scanner e radar, in modo da poter identificare e riconoscere i limiti della carreggiata ed eventuali ostali al fine di non compromettere la sicurezza delle persone; *Hyperloop*, progetto *open source* e basato su treni a levitazione magnetica in tunnel sottovuoto per viaggi a lunga distanza; Capsule per viaggi spaziali e per incentivare il turismo.

Tale scenario tecnologico sembra futuristico, ma diventerà reale nel 2031, e di conseguenza aumenterà anche la complessità delle minacce e che attualmente hanno accentuato la necessità di ulteriori sinergie e di una cooperazione più stratta a tutti i livelli della *smart city* (Infrastruttura e Reti, Sensoristica, *Delivery Platform*, Applicazione e Servizi). Molte delle attuali preoccupazioni in materia di sicurezza derivano dal fatto che tali minacce sono sempre più differenziate e internazionali, e hanno una natura sempre più transfrontaliera e intersettoriale. Richiedono quindi una risposta coordinata ed efficace.

Il rapporto Clusit 2023[1] evidenzia in Italia un notevole incremento del numero di attacchi registrati nel 2022. Il numero di incidenti rilevati è cresciuto significativamente con un aumento del 527%. La stragrande maggiorana degli attacchi si riferisce alla categoria "*Cybercrime*", che rappresenta il 93% del totale, +11% rispetto al resto del mondo. Uno scenario preoccupante, guardando anche la

[1] Rapporto clusit 2023, https://clusit.it/rapporto-clusit/.

distribuzione delle tecniche di attacco. Il malware è la matrice prevalente delle attività malevole svolte in Italia (53%), seguono con 8% attacchi di *Phishing* e *Social Engineering*, 6% vulnerabilità, e attacchi DDoS (*Distributed Denial of Services*) e furto d'identità rispettivamente con il 4% e 2%. Inoltre, per un 27% (*Unknown*) non è possibile identificare la tecnica primari di attacco.

Di conseguenza, la minaccia cyber può avere impatti devastanti sulla *smart city* ed in particolare sulla mobilità sostenibile, in quanto gli eventi cyber possono tradursi in impatti *physical*. Occorre quindi identificare ed annualizzare soluzioni volte non solo alla protezione delle infrastrutture IT (*Information Technology*) e OT (*Operational Technology*)[2] ma anche alla prevenzione e contenimento degli effetti che un attacco *Cyber* può avere sul mondo *Physical*. Questo richiede la stretta collaborazione tra tutti gli attori coinvolti per lo sviluppo della mobilità sostenibile. Infatti, l'industria automobilistica è nel mezzo di una trasformazione dirompente, che ha dato origine a tre tendenze in crescita: elettrificazione, guida autonoma e mobilità condivisa e intelligente. L'aumento della connettività gioca un ruolo fondamentale in queste tendenze in crescita, mentre la tecnologia avanza rapidamente per soddisfare la domanda di nuovi modelli di business automobilistici basati su servizi e funzionalità che migliorano la qualità creando esperienze di guida più sicure, più piacevoli e più efficaci. Nel frattempo, milioni di veicoli connessi sono schierati sulla strada in tutto il mondo ogni anno, con dispositivi e meccanismi che controllano l'accelerazione, lo sterzo e la frenata, tutti esposti ad attacchi informatici remoti, che mettono a rischio la privacy, la sicurezza del conducente e la continuità del servizio. Secondo *Upstream*, diversi sono i vettori di attacco che giocano un ruolo fondamentale sull'ecosistema della *smart mobility*: ECUs (*Electronic Control Units*), *Infotainment, Automotive* e *smart mobility* APIs, applicazioni mobile, *cloud*, *remote keyless*, EV charching. Durante il 2022, i ricercatori di Upstream's Auto Threat hanno analizzato 268 incidenti di sicurezza in ambito automotive e smart mobility, di cui il 63% erano attività malevole legate al *cybercrime*.

Inoltre, diverse sono le vulnerabilità identificate nei veicoli: 151 CVEs relative al 2022; 139 relative al 2021; 33 relative al 2020; ed infine 24 relative al 2019. Una CVE (*Common Vulnerability Exposure*) è un rischio di *cyber security* riconosciuto e catalogato in base al suo impatto. Nell'ecosistema automotive tale impatto è stato classificato su tre livelli in quanto sono state identificate vulnerabilità critiche, alte

---

[2] **Operational Technology**: hardware e software dedicati a rilevare o causare cambiamenti nei processi fisici attraverso il monitoraggio e / o il controllo diretto di dispositivi fisici quali valvole, pompe, ecc.. OT è l'uso di computer per monitorare o alterare lo stato fisico di un sistema, come il sistema di controllo di una centrale elettrica o la rete di controllo di un sistema ferroviario. Il termine si è affermato per dimostrare le differenze tecnologiche e funzionali tra i sistemi IT tradizionali e l'ambiente dei sistemi di controllo industriale esempi di OT includono: Sistemi di controllo industriale (ICS), sistemi di controllo di supervisione e acquisizione dati (SCADA), sistemi di controllo distribuito (DCS), Remote Terminal Unit (RTU) e controllori programmabili (PLC).

e medie. Sommer *et al.* (2019) per poter valutare tale impatto ed analizzare ulteriori minacce anno identificato una tassonomia basata su tre casi particolari: (i) *Incident management*, (ii) *Threat Analysis and Risk Assessment* (TARA), e (iii) *Security Testing*. Ciò permette non solo di adottare opportune contromisure in caso di incidente ma anche di poter definire nuovi attacchi all'interno del veicolo. Pertanto, la tassonomia presenta tre livelli di astrazione per consentire di categorizzare gli incidenti di sicurezza (Livello 1 di astrazione) nei sistemi noti, analizzarli e trasferirli al modello TARA per concretizzare le minacce attraverso una descrizione dettagliata (Livello 2) ed eseguire test di sicurezza sulle diverse componenti (Livello 3).

Al contempo, il modello STRIDE identificato da Microsoft consente di declinare le diverse tipologie di attacco in accordo alla seguente classificazione (Microsoft 2009; Dobaj *et al.* 2021):

- *Spoofing*: consiste nel falsificare determinate informazioni e utilizzare tale falsificazione per poter dialogare con l'utente (Falsificazione di Identità).
- *Tampering*: alterazione di un'informazione o codice software che si presuppone non sia oggetto di modifica (Alterazione dei dati).
- *Repudation*: dichiarare di non aver fatto qualcosa, indipendentemente dal fatto che sia stato eseguito o meno. Ad esempio, un utente compie un'azione illegale sul sistema e il sistema non è in grado di rilevare l'azione o identificare l'utente (Ripudio di una azione).
- *Information Disclosure*: coinvolge l'esposizione di informazioni ad individui che non hanno permessi di accesso (Divulgazioni di informazioni).
- *Denial of Service (DoS)*: insieme di attacchi che mirano all'interruzione di un servizio. Questi includono come effetto il *crashing*, il rallentamento che porta alla non usabilità del sistema e il riempimento degli *storage* (Diniego del servizio).
- *Elevation of privilege*: avviene nel momento in cui un utente o programma riesce ad ottenere dei privilegi non previsti per il suo ruolo (Elevazione dei privilegi).

Tali modelli, possono essere utili per l'identificazione degli attacchi e delle minacce su diversi componenti dei veicoli moderni [23]:

- *On-board Diagnostic Port (OBD)*: montata su tutti i veicoli ed utilizzata come diagnostica. Essa non sempre implementa meccanismi di autenticazione e cifratura, quindi, può essere sfruttata per inviare/ricevere messaggi.
- *Electronic Control Unit (ECU)*: un sistema embedded che controlla altri sottosistemi del veicolo.
- *Controller Area Network (CAN)*: protocollo ampiamente utilizzato e di cui abbiamo già discusso.
- *Sensori* (presenti nei più recenti veicoli):
    - *Light Detection And Ranging (LiDAR)*: sensori che usano la luce per misurare la distanza da un determinato oggetto.

  - *Radio Detection and Ranging (Radar)*: sensori che inviano segnali elettromagnetici per rilevare oggetti e misurare la loro distanza.
  - *Global Positioning System (GPS)*: sistema di navigazione satellitare.
  - *Telecamere*: applicate ai veicoli, forniscono informazioni sul traffico e possono essere usate anche dai veicoli a guida autonoma.
- *Meccanismi di connessione*: cellulari, Bluetooth, *Wireless Access in Vehicular Environments* (WAVE) e Wi-Fi.

Inoltre, possiamo suddividere gli attacchi anche in remoti o fisici:

- *Attacchi ad accesso remoto*: possono essere eseguiti a distanza senza dover accedere fisicamente al veicolo. Alcuni esempi includono la modifica dei messaggi e di inviare messaggi contraffatti, bloccare segnali e collezionare dati confidenziali.

Attacchi fisici: attacchi che possono essere effettuati soltanto tramite un accesso fisico al veicolo, ad esempio, tramite OBD-II. Altri attacchi riguardano anche la compromissione delle ECU tramite tecniche di *reverse engineering*. Sfruttando questo, se vengono individuate ulteriori vulnerabilità, è possibile sfruttare attacchi remoti.

Best Practice

Considerando la necessità di collaborazione tra i vari stakeholder che concorrono alla realizzazione della smart city e le micacce *cyber* e *physical* identificate nell'ecosistema *smart mobility*, è necessario identificare metodi, tecniche e strumenti capaci di operare una gestione cyber-fisica del rischio lungo tre dimensioni:

- *Detection*: associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica.
- *Response*: associata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica viene rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica.

Prevention: associata alla definizione e attuazione delle attività per la gestione dei piani e per il ripristino dei processi e dei servizi impattati da un incidente.

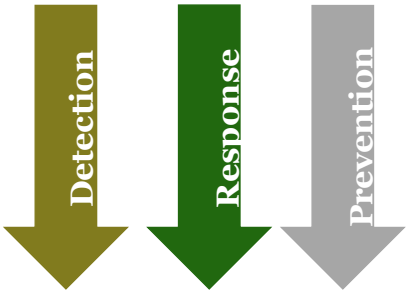


Figura 1: Dimensione vertical (Cybersecurity)

Ogni dimensione implementa i controlli di sicurezza implementati nell'*Hack Space* (Baldassarre *et al.* 2019) e che si rifanno ai controlli "CIS" definiti dal "Center for Internet Security[3]". Il Center for Internet Security è una organizzazione senza fini di lucro che ha l'obiettivo di identificare, sviluppare, promuovere e sostenere le "best practices" nel settore della cyber sicurezza; fornire soluzioni a livello globale per prevenire e rispondere in modo rapido in caso di incidenti informatici; realizzare e guidare la comunità per rendere il cyberspazio più sicuro.
I controlli CIS sono una serie di azioni prioritarie che costituiscono nel loro insieme una serie di "*best practices*" difensive che mitigano gli attacchi più comuni contro i sistemi e le reti. I controlli CIS sono sviluppati da una comunità di esperti IT che applicano la loro esperienza alla difesa informatica.

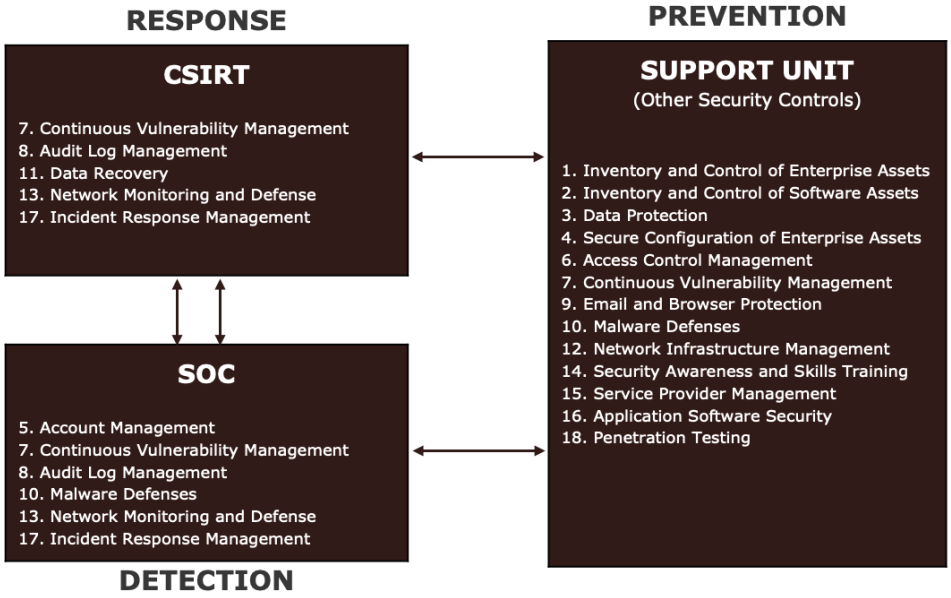


Figura 2: The Hack-Space Model

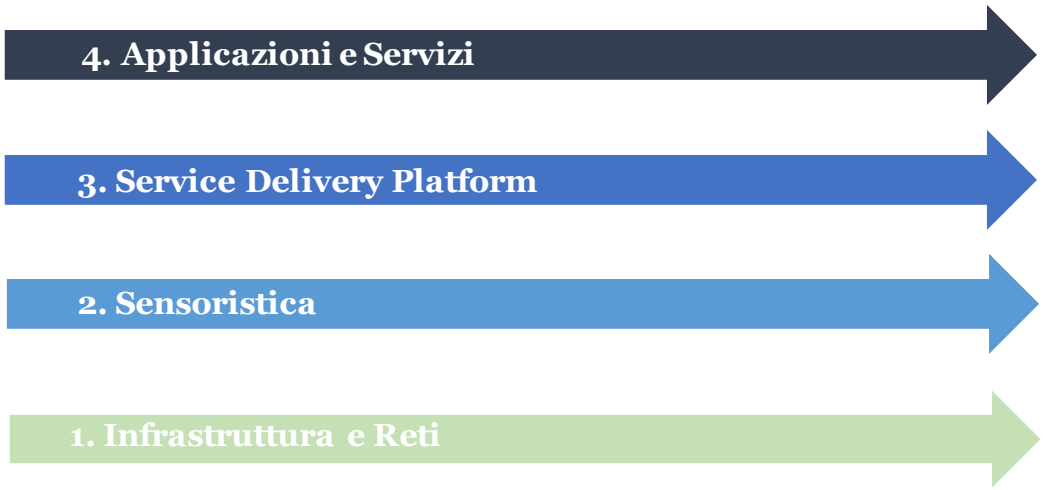
Tali dimensioni di sicurezza possono essere declinate nella dimensione verticale di una smart city per poter orchestrare e gestire opportunamente la sicurezza della smart mobility lungo i quattro strati tecnologici:

1. *Infrastruttura e Reti*: reti e dotazioni tecnologiche abilitanti la costruzione di una Smart City (*layer 1*).
2. *Sensoristica*: strato realizzato da dispositivi IoT (Internet of Things) che hanno sensori, software e altre tecnologie integrate allo scopo di connettere e scambiare dati con altri dispositivi e sistemi su Internet (*layer 2*).
3. *Service Delivery Platform*: piattaforme in grado di elaborare e valorizzare i big data del territorio e raccolti dai livelli sottostanti (*layer 3*).

[3] Center for Internet Security, https://www.cisecurity.org.

4. *Applicazioni e Servizi*: strato di applicazioni e servizi che rappresentano l'interfaccia con gli utenti finali (*layer 4*).

Figura 3: Dimensione orizzontale (Strati tecnologici)



L'obiettivo è quello di fornire una visione integrata dei servizi offerti dai livelli tecnologici della smart mobility, ponendo l'attenzione su una gestione sicura di tali livelli.

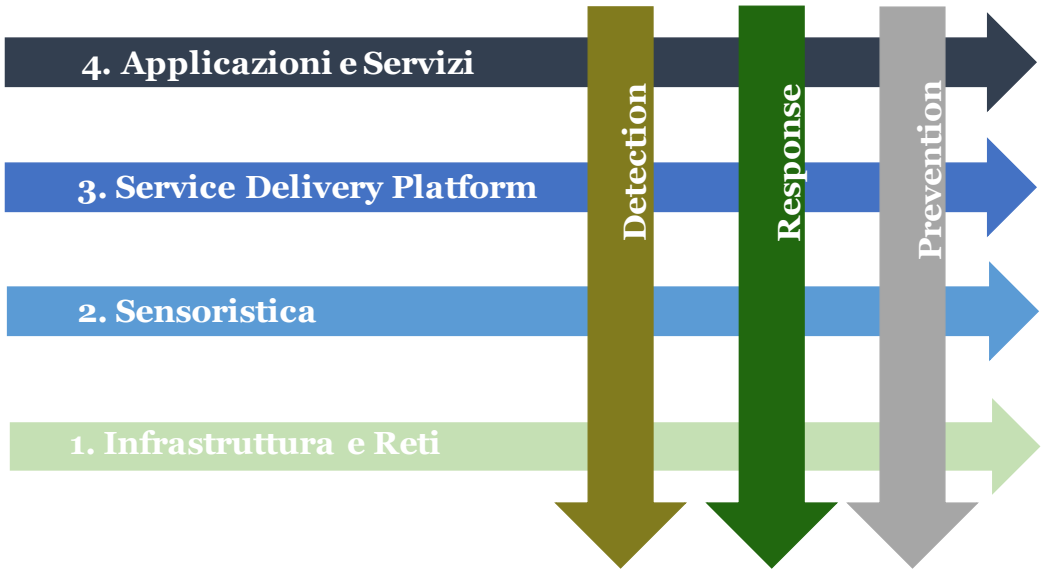


Figura 4: Secure Smart Mobility

Bibliografia

Al Sharif R. (2022). Smart City Dimensions and Associated Risks: Review of literature, *Sustainable Cities and Society*, 77, pp. 1-14. 10.1016/j.scs.2021.103542.

Aletà N. B., Alonso C. M. e Ruiz R. M. A. (2017). Smart Mobility and Smart Environment in the Spanish cities, *Transportation Research Procedia*, 24, pp. 163-170. 10.1016/j.trpro.2017.05.084.

Allam Z. e Newman P. (2018). Redefining the smart city: Culture, metabolism and governance, *Smart Cities*, 1 (1), pp. 4-25. 10.3390/smartcities1010002.

Baldassarre M. T., Barletta V. S., Caivano D., Raguseo D., Scalera M. (2019). Teaching Cyber Security: The HACK-SPACE Integrated Model, in P. Degano e R. Zunino (a cura di), *ITASEC19*, Vol. 2315.

Batty M. (2013). Big data, smart cities and city planning, *Dialogues Hum Geogr*, 3 (3), pp. 274–279. 10.1177/2043820613513390.

Dobaj J., Macher G., Ekert D., Riel A. e Messnarz R. (2021). Towards a security-driven automotive development lifecycle, *Journal of Software: Evolution and Process*, SPECIAL ISSUE - METHODOLOGY PAPER, pp. 1-22. 10.1002/smr.2407.

EY e IIA (2021). *Move to the future: la mobilità del 2031*, EY and IIA.

Garcia M. H. C. et al. (2021). A Tutorial on 5G NR V2X Communications, *IEEE Communications Surveys and Tutorials*, 23 (3), pp. 1972-2026. 10.1109/COMST.2021.3057017.

Manyika J., Chui M., Brown B., Bughin J., Dobbs R., Roxburgh C. e Hung Byers A. (2011). *Big data: The next frontier for innovation, competition, and productivity*, McKinsey Global Institute.

Mayer-Schönberger V., Cukier K. N. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Boston: Houghton Mifflin Harcourt.

Mir U., Abbasi U., Mir T., Kanwal S. e Alamri S. (2021). Energy Management in Smart Buildings and Homes: Current Approaches, a Hypothetical Solution, and Open Issues and Challenges, *IEEE Access*, 9, pp. 94132-94148. 10.1109/ACCESS.2021.3092304.

Olson N. (2016). The Internet of things, *New Media Soc*, 18 (4), pp. 680-682. 10.1177/1461444815621893a.

Pham M. e Xiong K. (2021). A survey on security attacks and defense techniques for connected and autonomous vehicles, *Computer & Security*, 109, pp. 102269-102373. 10.1016/j.cose.2021.102269.

Rahman M. W., Islam R., Hasan A., Bithi N. I., Hasan M. M. e Rahman M. M. (2022). Intelligent waste management system using deep learning with IoT, *Journal of King Saud University - Computer and Information Sciences*, 34 (5), pp. 2072-2087. 10.1016/j.jksuci.2020.08.016.

Smith M., Miller S. (2022). The ethical application of biometric facial recognition technology, *AI Soc*, 37 (1), pp. 167–175. 10.1007/s00146-021-01199-9.

Sommer F., Dürrwang J. e Kriesten R. (2019). Survey and classification of automotive security attacks, *Information*, 10 (4), pp. 1-29. 10.3390/info10040148.

Taylor P. J., Dargahi T., Dehghantanha A., Parizi R. M. e Choo K. K. R. (2020). A systematic literature review of blockchain cyber security, *Digital Communications and Networks*, 6 (2), pp. 147-156. 10.1016/j.dcan.2019.01.005.

Thaseen Ikram S., Mohanraj V., Ramachandran S. e Balakrishnan A. (2023). An Intelligent Waste Management Application Using IoT and a Genetic Algorithm–Fuzzy Inference System, *Applied Sciences (Switzerland)*, 13 (6). 10.3390/app13063943.

Uganya G., Rajalakshmi D., Teekaraman Y., Kuppusamy R. e Radhakrishnan A. (2022). A Novel Strategy for Waste Prediction Using Machine Learning Algorithm with IoT Based Intelligent Waste Management System, *Wirel Commun Mob Comput*, pp. 1-15. 10.1155/2022/2063372.

Umair M., Cheema M. A., Cheema O., Li H., Lu H. (2021). Impact of COVID-19 on iot adoption in healthcare, smart homes, smart buildings, smart cities, transportation and industrial IoT, *Sensors*, 21 (11), pp. 1-33. 10.3390/s21113838.

Yaga D., Mell P., Roby N. e Scarfone K. (2018). *Blockchain technology overview*, Nistir 8202. 10.6028/NIST.IR.8202.

Yan L., Sheng M., Wang C., Gao R. e Yu H. (2022). Hybrid neural networks based facial expression recognition for smart city, *Multimed Tools Appl*, 81 (1), pp. 319–342. 10.1007/s11042-021-11530-7.

Zaheer T., Malik A. W., Rahman A. U., Zahir A. e Fraz M. M. (2019). A vehicular network–based intelligent transport system for smart cities, *International Journal of Distributed Sensor Networks*, 15 (11), pp. 1-13. 10.1177/1550147719888845.