

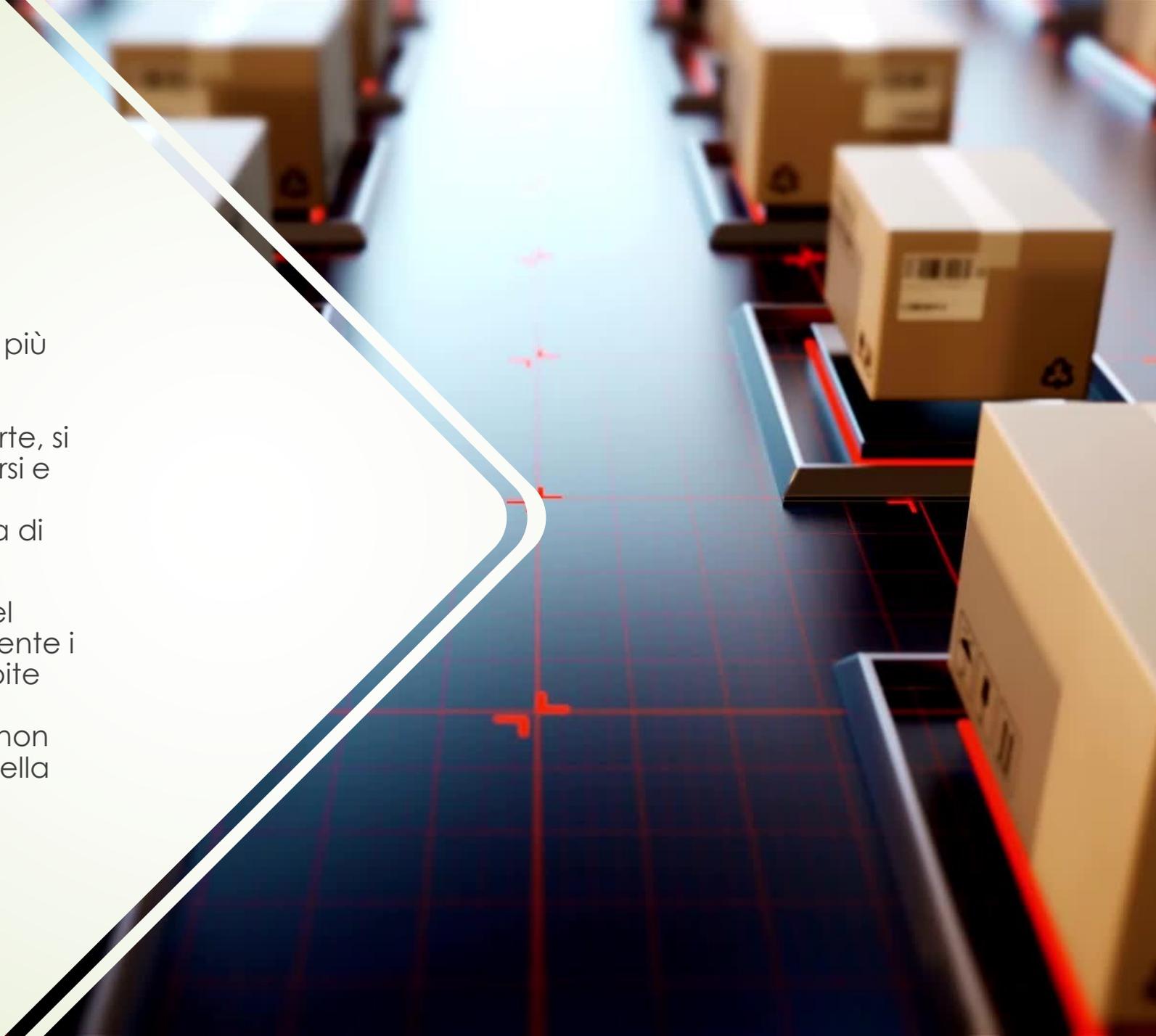


Sicurezza



Sicurezza

- Il cybercrime rappresenta la categoria più temuta nella scala evolutiva dei rischi. Definito chi colpire e quali sono le sue debolezze, l'azione di penetrazione parte, si prende il tempo necessario per insediarsi e agire, per generare quella che si può definire una "cyber-estorsione". Si tratta di un fenomeno in crescita.
- Paradossalmente, l'entrata in vigore del GDPR potrebbe incoraggiare ulteriormente i malintenzionati, poiché le aziende colpite (e mal protette) potrebbero preferire il pagamento di un riscatto (comunque non trascurabile) all'esposizione pubblica della segnalazione, resa necessaria dalla normativa.



Sicurezza

- La soluzione si basa su agenti implementati sugli host (capofila) dell'infrastruttura da monitorare. Gli eventi rilevati vengono indirizzati verso un motore analitico che, utilizzando modelli di machine learning, esplora nel data base delle minacce già catalogate, evidenzia i rischi e suggerisce misure di intervento.
- Sempre più imprese stanno incrementando gli investimenti in sistemi di **intelligenza artificiale** per difendersi dagli attacchi informatici di nuova generazione. A dirlo è il nuovo studio del **Capgemini Research Institute**. Due terzi (69%) delle imprese riconoscono di non essere in grado di rispondere alle minacce critiche senza il supporto dell'AI.



Sicurezza

- ▶ Sono notevolmente aumentati i tipi di attacchi informatici che richiedono un intervento immediato o che i cyber analyst non sono in grado di risolvere abbastanza rapidamente
- ▶ Le aziende si trovano ad affrontare un volume e una complessità di minacce informatiche senza precedenti e si sono rese conto dell'importanza dell'AI come primo elemento di difesa



Sicurezza

- ▶ In merito alla difesa dai crimini comuni (non informatici) la previsione del crimine in tempo reale, con l'intelligenza artificiale, è oggi una priorità per la comunità scientifica che si impegna a sviluppare modelli statistici sempre più precisi ed efficaci.
- ▶ Gli obiettivi degli esperti incaricati di sviluppare gli algoritmi riguardano in primis l'individuazione di luogo e tempo di un probabile crimine. In secondo luogo, si concentrano su causa e vittima.



Sicurezza

- ▶ *“Signor Marks, in nome della sezione Precrimine di Washington, la dichiaro in arresto per il futuro omicidio di Sarah Marks e Donald Dubin, che avrebbe dovuto avere luogo oggi 22 Aprile alle ore 8 e 04 minuti”.*
- ▶ *-Dal film: “Minority Report”, 2002, Steven Spielberg*

I dipartimenti di polizia che utilizzano l'analisi predittiva per la prevenzione del crimine sono attivi nelle nostre città da anni.



Sicurezza

E' possibile dividere le **tecniche predittive** in quattro classi:

- La prima è composta dalle **tecniche di analisi statistica classiche**, che utilizzano modelli multivariati basati su regressioni, oltre a modellistica basata sulle *time-series* con procedure di destagionalizzazione annesse.
- La seconda classe include i **metodi semplici**, che sono quelli che non richiedono un'ampia mole di dati o un processo complesso di calcolo: ad esempio i metodici euristici basati su indici e *checklists* piuttosto che su *big data*.

Sicurezza

- La terza classe è formata dalle cosiddette **applicazioni complesse**, le quali richiedono oltre che un numero considerevole di dati analizzabili anche nuove e sofisticate tecniche computazionali
- La quarta classe comprende i **metodi personalizzati**, che non sono nient'altro che metodi statistici e tecniche già sperimentate che vengono adattate a modelli più specifici di supporto alla polizia predittiva. Per esempio modelli e metodi di machine learning utilizzati per creare *heat maps* (mappe che scottano)
- I modelli analitici basati sul **near-repeat** consentono di **predire il luogo** del crimine in un futuro molto prossimo

Sicurezza

- **Per predire il momento** in cui un'azione criminale ha probabilità di essere compiuta risulta plausibile utilizzare due categorie analitiche differenti: l'**analisi spazio temporale** (utilizza i dati storici dei crimini e i dati temporali creando dei modelli di predizione come le *heat maps*) oppure basarsi su **dati geografici associati al rischio** creando modelli predittivi geo-spaziali.
- **Gli hot spot (le "zone calde")** appaiono grazie all'incrocio tra dati storici sui reati e altre variabili.

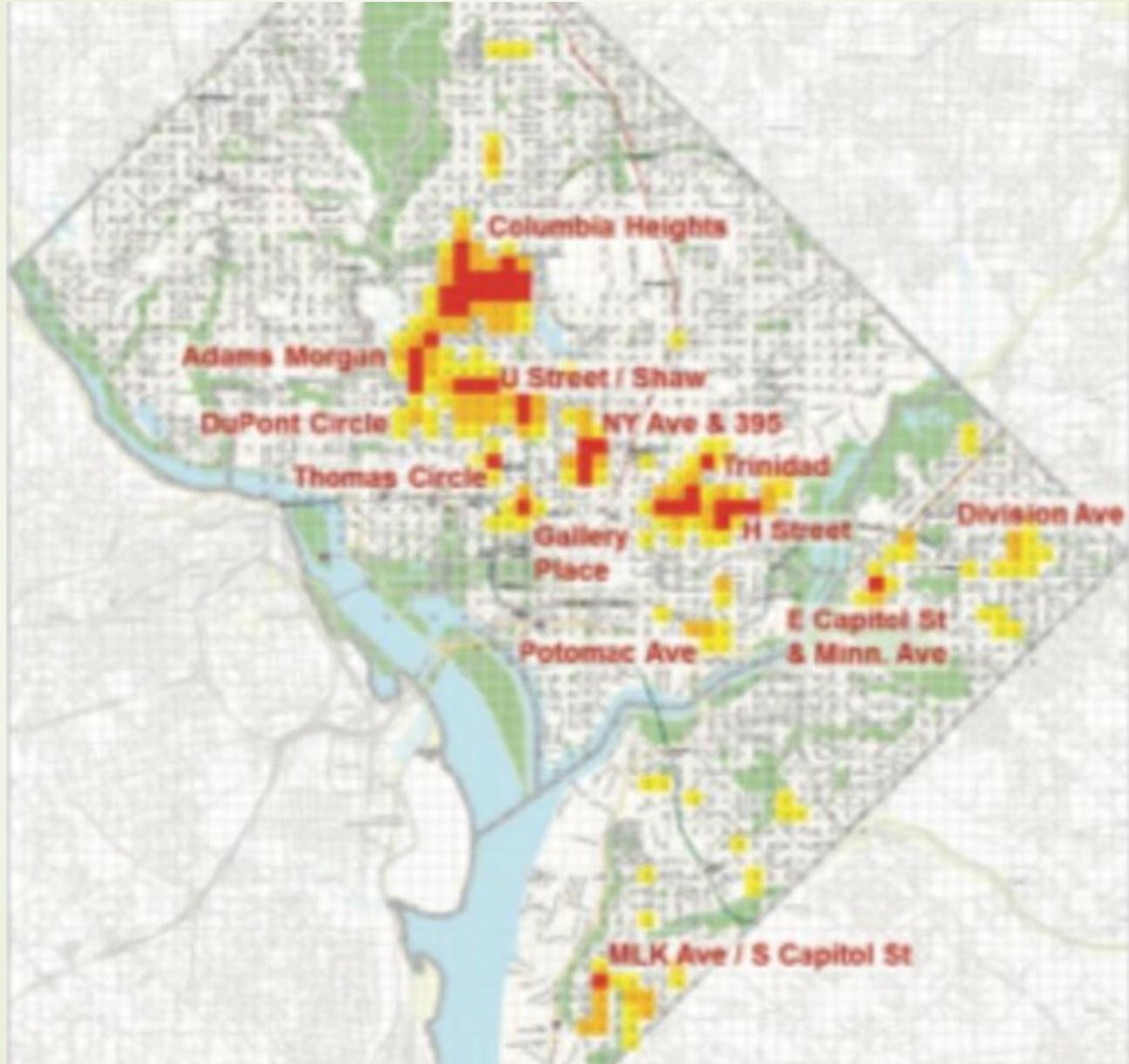
$$F = G \frac{m_1 m_2}{d^2}$$

$$\frac{\partial}{\partial t} \psi = -\hat{H} \psi$$

$$\phi(x) = \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{x^2}{2\sigma^2}}$$

$$E = mc^2$$

$$\frac{df}{dt} =$$



Sicurezza

- ▶ Il software PredPol venne sviluppato nel 2013 grazie alla collaborazione tra il dipartimento di polizia di Los Angeles, l'Università di Santa Clara e l'Università della California: funziona tramite un solo algoritmo di *machine learning*.
- ▶ I *dataset* messo a disposizione per la predizione utilizza dati storici (vecchi dai due e i cinque anni) e le variabili tenute in considerazione dal modello sono solamente tre: data, ora e luogo del crimine, tipologia di crimine commesso.
- ▶ Le predizioni vengono proiettate e visualizzate tramite un'**interfaccia messa a disposizione da Google Maps** che mette in luce gli *hot spot*, disegnando direttamente sulla mappa quadrati rossi di 150 m² l'uno.

Sicurezza

- ▶ A Genova i primi test (maggio 2019) di servizi dedicati al controllo e al monitoraggio del territorio attraverso l'uso di **droni** controllati da remoto sfruttando il **5G**.
- ▶ La sperimentazione, che ha avuto luogo nell'area del Great Campus agli Erzelli, dove ha sede il Digital Lab 5G e uno dei centri R&S globali di **Ericsson** in Italia, si avvale di una centrale operativa in Cloud realizzata da **Tim**, dalla quale è possibile gestire e controllare in modo automatizzato le varie missioni di volo.



Sicurezza

- ▶ Droni in grado di volare autonomamente senza il bisogno dell'intervento umano da utilizzare in situazioni di emergenza, come la ricerca di persone disperse o il monitoraggio di incendi: questi gli obiettivi di UAV RETINA, iniziativa europea.
- ▶ Il progetto prevede droni dotati di sensori che raccolgono **immagini nello spettro visibile e immagini termiche** da inviare a un sistema informatico che le analizza, estrapolando gli elementi utili ai soccorritori, per prendere decisioni più rapide e allo stesso tempo efficaci. In qualsiasi momento, un telepilota certificato può assumere il pieno controllo del drone per evitare che sorvegli aree indesiderate

