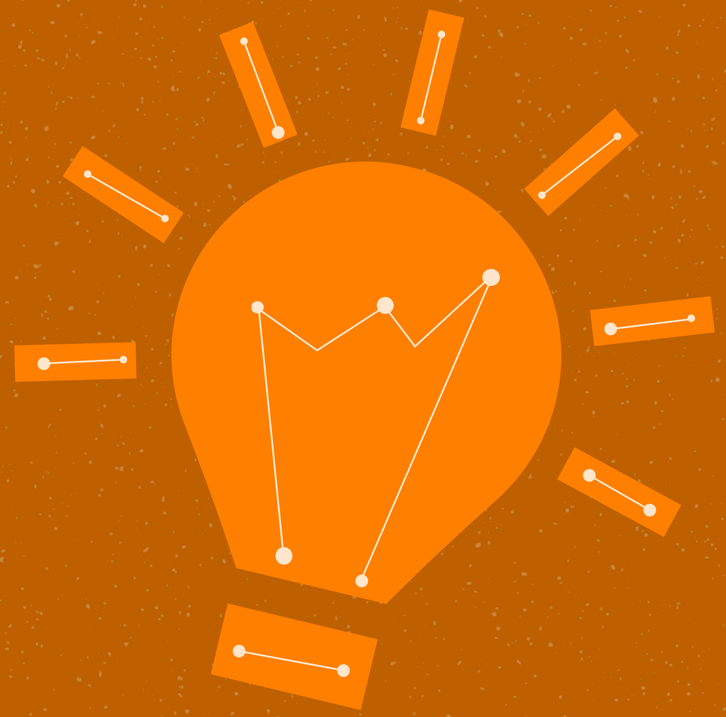
Puglia

OSSERVAZIONI SUL FUTURO



Le Competenze per la Cybersecurity e lo Stato della Ricerca

Prof. **Donato Malerba**
Dipartimento di Informatica,
Università degli Studi di Bari Aldo Moro

Bari, 20 10 2022

NUOVA FIERA DEL LEVANTE
UNIONE EUROPEA
PUGLIA FESR·FSE 2014/2020 Il futuro alla portata di tutti
REGIONE PUGLIA

Cybersecurity

Google Trends

Query associate	In aumento
1 agenzia cybersecurity	Impennata
2 agenzia nazionale cybersecurity	Impennata
3 hacker	Impennata
4 master cyber security	Impennata
5 cybersicurezza	Impennata

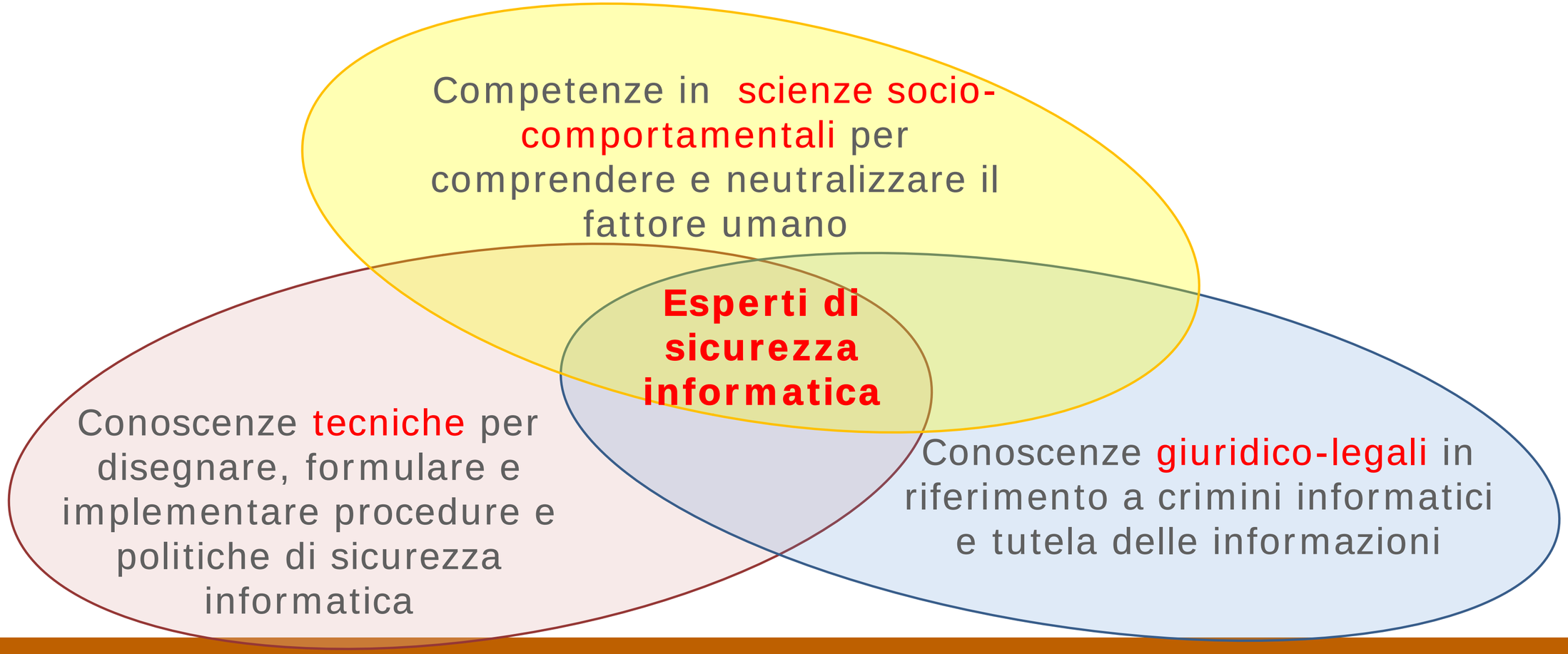
Argomenti correlati	In aumento
1 Agenzia governativa - Tipo di organizzazione	Impennata
2 Hacker - Argomento	Impennata
3 Laurea magistrale - Laurea	Impennata
4 Exchange-traded fund - Argomento	Impennata
5 Software - Argomento	Impennata

per regione

1	Lazio
2	Piemonte
3	Lombardia
4	Puglia
5	Friuli-Venezia Giulia

Cybersecurity

Competenze richieste: una sfida interdisciplinare



Cybersecurity

Formazione specialistica

- Il Report – Addressing Skills Shortage and Gap Through Higher Education - evidenzia nel 2021 la buona prestazione dell'Italia, seconda dopo la Spagna in ambito Unione Europea, nell'attivare programmi universitari dedicati alla sicurezza informatica

- Sul totale dei corsi Europei, 97 (ossia il 77%) sono corsi Universitari e post-Universitari, tuttavia ENISA raccomanda di *attuare i programmi di formazione alla cybersecurity già durante la scuola secondaria*

Cybersecurity

Formazione specialistica

- Sfida: la forte **dinamicità** e **mutevolezza** dell'ambiente cyber stabilisce requisiti elevati per la consapevolezza, le competenze e le abilità della forza lavoro.
- Nella ECS EUROPEAN CYBER SECURITY ORGANISATION (European Cyber Security Organisation), che accoglie 270 partner industriali e di ricerca, il tema è affrontato in
  - WP5: "Education, Awareness, Training, and Cyber Ranges"
  - TF "European Human Resources Network for Cyber" (EHR4CYBER).

  Linee guida: *"European Cybersecurity Education and Professional Training: Minimum Reference Curriculum"*

Cybersecurity

Formazione specialistica

Linee guida: *“European Cybersecurity Education and Professional Training: Minimum Reference Curriculum”*

- Rivolte a studenti di sicurezza informatica, istituti di istruzione superiore, professionisti, fornitori di formazione professionale e sviluppo della forza lavoro e datori di lavoro.
- Colma il **divario** tra industria e mondo accademico nello sviluppo delle capacità e delle competenze della forza lavoro della sicurezza informatica.

Cybersecurity

Formazione specialistica

Il curriculum è organizzato in una struttura semplificata e consolidata all'interno dei cluster di competenze di base, intermedi e avanzati.

Cybersecurity Principles and Management

- ICT Infrastructure and Security
- Cybersecurity Principles
- Information and Cybersecurity Management/Decision-making
- Cybersecurity Project Management

Cybersecurity Tools and Techniques

- Information Systems Security
- Enterprise Cybersecurity Practice
- Network and Applications Security
- Vulnerability Assessment & Threat Management

Cybersecurity in Emerging Digital Technologies

- Cybersecurity for AI
- Machine Learning Security
- Cybersecurity for Emerging Cloud Technologies
- Cybersecurity for the Digital Transformation
- Cybersecurity and Digital Era Leadership

Offensive Cybersecurity Practitioners

- Ethical Hacking and Offensive Cybersecurity
- Cybersecurity and Cyber Ranges in Practice
- Cybersecurity Forensics / Threat Intelligence
- Internet of Things(IoT) Cybersecurity Practitioner

Cybersecurity

Formazione specialistica @ Dipartimento di Informatica, UNIBA

Corso di Laurea Magistrale in Sicurezza Informatica (Taranto), attivo dal 2017, per la formazione di laureati in grado di:

- collaborare all'analisi e alla valutazione tecnica dello stato di sicurezza di un sistema informatico
- supportare la progettazione, realizzazione, gestione e manutenzione di sistemi sicuri
- gestire dati sensibili in contesti pubblici e privati
- gestire il rischio derivante da falle di sicurezza
- usare tecniche di analisi dei dati per scoprire e mitigare falle nella sicurezza

Cybersecurity

Formazione specialistica @ Dipartimento di Informatica, UNIBA

Corso di Laurea Magistrale in Computer Science (Bari) Curriculum in Security Engineering attivo dal 2021, per la formazione di laureati con competenze relative agli aspetti avanzati di:

- progettazione affidabile, sicura e performante del software e dei sistemi
- programmazione sicura
- progettazione dell'interazione in sistemi sicuri, degli oggetti che comunicano tra di loro e/o con le persone
- analisi di immagini e video per la sicurezza urbana
- sintesi e uso di tecniche di intelligenza artificiale in cybersecurity

Cybersecurity

Formazione post-universitaria @ Dipartimento di Informatica, UNIBA

- Accordo con il Joint Research Centre JRC della Commissione Europea (*Collaborative Doctoral Partnership*) per il dottorato di ricerca in Informatica e Matematica sui temi della IA in cybersecurity.

- Borse di dottorato di ricerca finanziate dall'Università degli Studi di Bari e dal **Programma PON RI 2014-2020 e PNRR** su temi di cybersecurity nell'ambito della Intelligenza Artificiale, Trattamento di dati Sensibili, Sicurezza e Privacy del Software, Automotive Security

Cybersecurity

Formazione specialistica e altro @ Dipartimento di Informatico UNIBA

- Corso per l'acquisizione di competenze trasversali in Cyberchallenge per studenti universitari e dipendenti di organizzazioni pubbliche e imprese

- Partecipazione dal 2019 al programma CYBER CHALLENGE.IT aperto a studenti di scuola superiore e università per la formazione delle nuove generazioni di cyber-defender

CYBERSECURITY NATIONAL LABORATORY

Cybersecurity

Formazione specialistica e altro @ Dipartimento di Informatico UNIBA

- Tutto questo con grande attenzione al bilancio di genere:

WOMEN 4CYBER™
EUROPEAN CYBER SECURITY ORGANISATION

Cybersecurity

Stato e direzioni della ricerca

Il Report ENISA (europa.eu) – Direction's of EU's Digital Strategic Autonomy – identifica nel 2021 le seguente aree chiave della ricerca:

- Sicurezza dei dati
- Piattaforme di trustworthy software
- Gestione e mitigazione delle minacce cyber
- Piattaforme di trustworthy hardware
- Crittografia
- Pratiche e strumenti centrati sull'utente
- Sicurezza nella comunicazione digitale

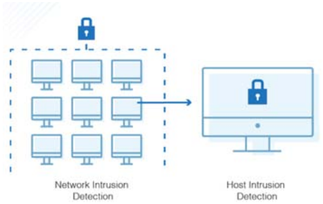
Cybersecurity

Stato e direzioni della ricerca

La priorità della ricerca in cybersecurity è la sicurezza dei dati con enfasi sulla privacy e la protezione di dati negli algoritmi e la sicurezza della intelligenza artificiale – gli hacker possono usare risultati dell'intelligenza artificiale (IA) per creare minacce alla sicurezza

Cybersecurity

IA pietra miliare della cybersecurity



SCOPERTA DI MINACCE NELLA RETE

- *Analizzare* grandi volumi di traffico di rete (interni ed esterni) e *identificare* pattern che sono parte di un incidente nella sicurezza
  - ✓anomalie nel comportamento degli utenti o negli eventi
  - ✓correlare le caratteristiche del traffico a note firme di attacco

ANALISI DELLE EMAIL

- *Classificare* email per scoprire *spam*, *malware*, tentativi di *phishing* nei messaggi email
  - ✓Classificazione
  - ✓Analisi di immagini
  - ✓Analisi del linguaggio naturale

SICUREZZA DELLE APPLICAZIONI

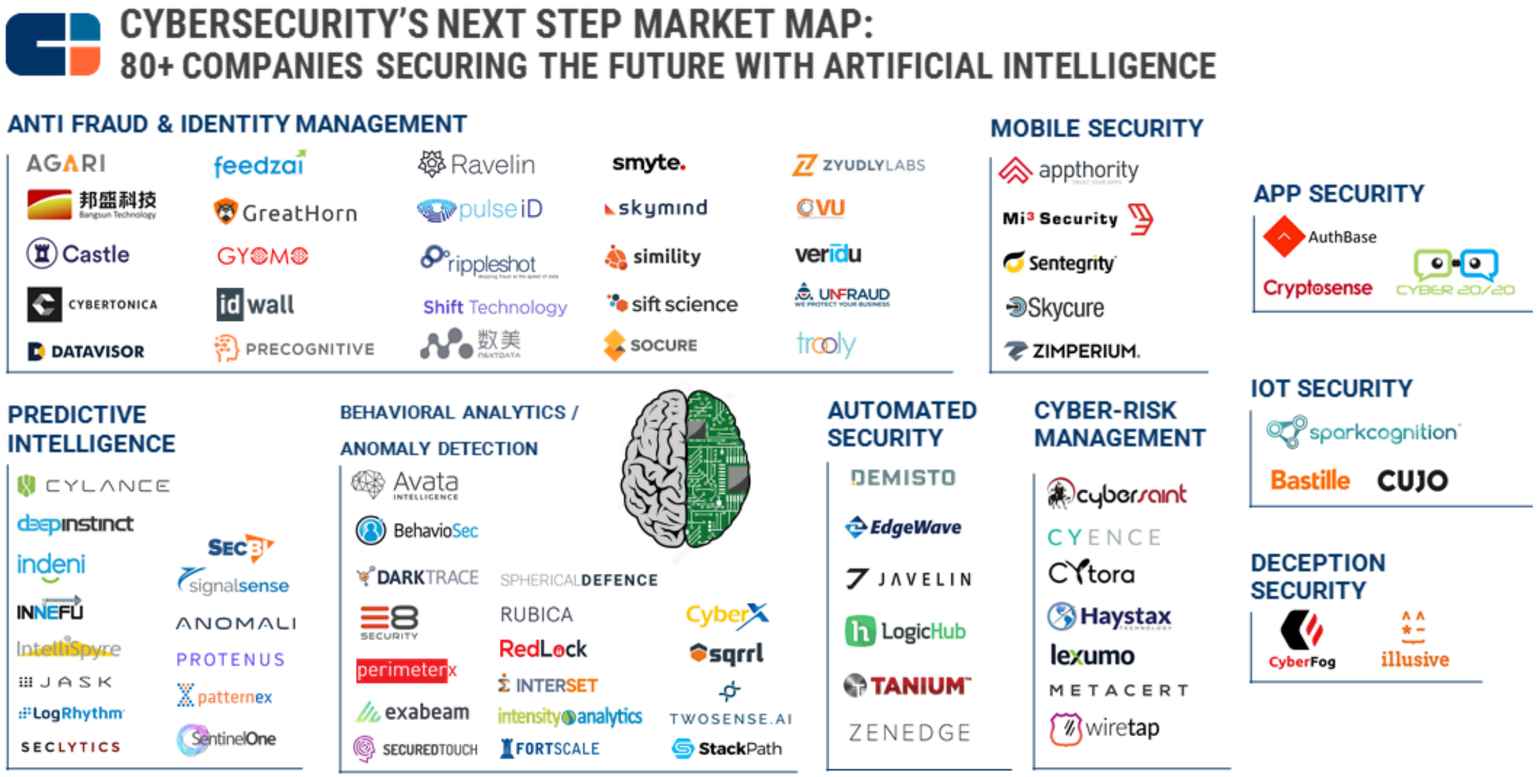
- Scoprire traffico/comportamento anomalo ed eventualmente bloccarlo o rispondere
- Identificare accessi non autorizzato o abuso di privilegi
- Scoprire vulnerabilità tramite analisi statica o dinamica del software

ANTI-VIRUS

- Classificare software sulla base della analisi statica del codice sorgente o comportamento del software
  - ✓Scoprire zero-day malware e mutazioni

Cybersecurity

IA nel cyber-mercato



https://www.cbinsights.com/research/cybersecurity-artificial-intelligence-startups-market-map/

Cybersecurity

Il lato oscuro dell’IA

Creazione di malware
Aumentare la capacità di evasione

Classificazione delle vittime
Ottimizzazione dell’attacco

Attacchi di phishing

Adversarial learning per attaccare e per difendere sistemi di IA

Cybersecurity

Diritto alla spiegazione

Fairness

Transparency

Privacy

Explainability

Un'organizzazione che usa dati per elaborazioni automatiche deve spiegare come il sistema automatico prende le decisioni[1]

1. Articolo 15(1)(h) Recital 71 del GDPR

Cybersecurity

Explainability in Cybersecurity

- Spiegare i cambiamenti (e.g., Andresini et al., 2021)
- Spiegare le decisioni dei modelli (e.g., Mahbooba et al., 2021; Alezeni et al., 2021; Dattaraj et al., 2021; Andresini et al., 2021; Caforio et al., 2021; Andresini et al., 2022)
- Spiegare come cambia il comportamento di diversi algoritmi (e.g, Al-Essa et al., 2021; Al- Essa et al., 2022; Al-Essa et al. (B), 2022;)
- Migliorare l'accuratezza delle decisioni (e.g., Al- Essa et al., 2022; Al-Essa et al. (B), 2022; Caforio et al., 2021; Andresini et al., 2022)
- Trovare le segnature di cyber-minacce (e.g., Mahbooba et al., 2021; Iadarola et al. 2021; Caforio et al., 2021) (e.g., Al- Essa et al., 2022; Al-Essa et al. (B), 2022; Fidel et al., 2019)
- Attaccare sistemi di cybersecurity (e.g., Kuppa et al., 2021)

Cybersecurity

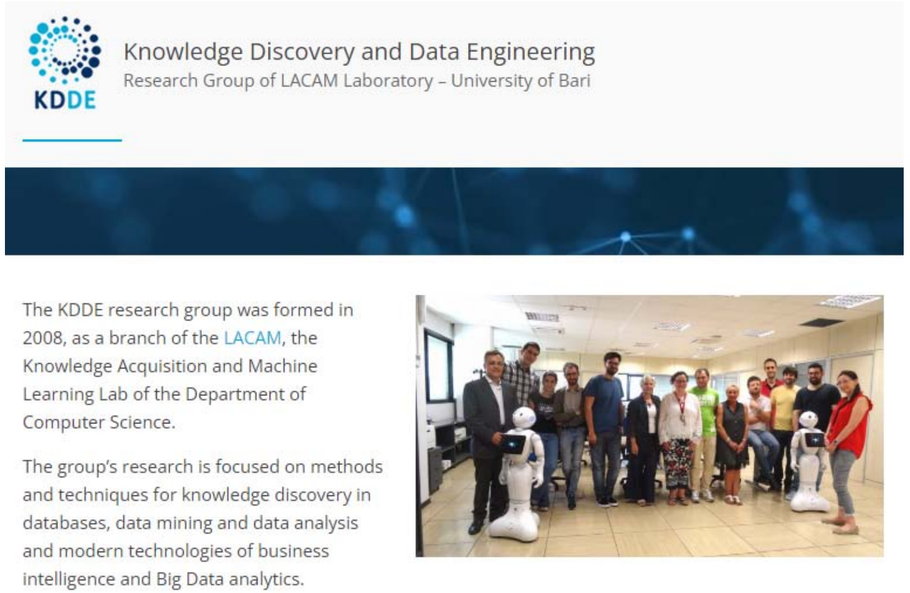
Cybersecurity @KDDE.di.uniba.it

KDDE

Tra IA, adversarial learning ed Explainable Artificial Intelligence

Parternariato esteso 01
IA: Aspetti fondazionali
Spoke di

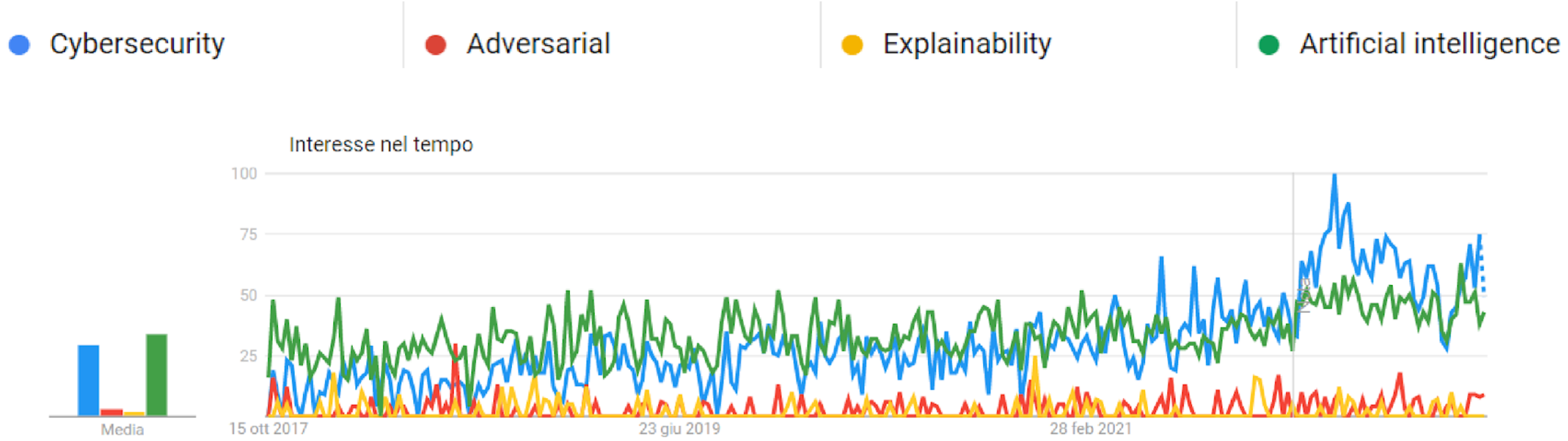
FUTURE AI RESEARCH



Parternariato esteso 07
Cybersecurity,
nuove tecnologie
e tutela dei diritti
partner di
SERICS – **Se**curity and **Ri**ghts in **C**yber **S**pace

Cybersecurity

Futuro della ricerca in Cybersecurity



Grazie per l'attenzione

Seguici su
https://www.facebook.com/KDDEdib/