IST 110: INFO, PEOPLE & TECH FALL 2024

L08:OSINT

GROUP MEMBERS:

REGINA LUNA, MPHO NKWANA & STEVEN WANG

WHAT IS **OSINT?**

Open Source Intelligence (OSINT) is the practice of collecting and analyzing information from publicly available sources like websites, social media, news, academic articles, think tank data and public records to gain insights on specific topics, individuals or events.

SOCIAL MEDIA OSINT -STEVEN

Social media OSINT involves the systematic collection and analysis of publicly available information from social media platforms.

Social Media OSINT

Collection and analysis of publicly available information

Uses platform-specific public APIs (e.g., Facebook, Instagram, Twitter)

Aggregated data reflects public opinions and trends

Social Media Intelligence (SOCMINT)

Involves both public and restricted information

Accesses data intended for specific audiences (e.g., private groups)

Can provide more targeted insights

SOCIAL MEDIA OSINT TECHNIQUES

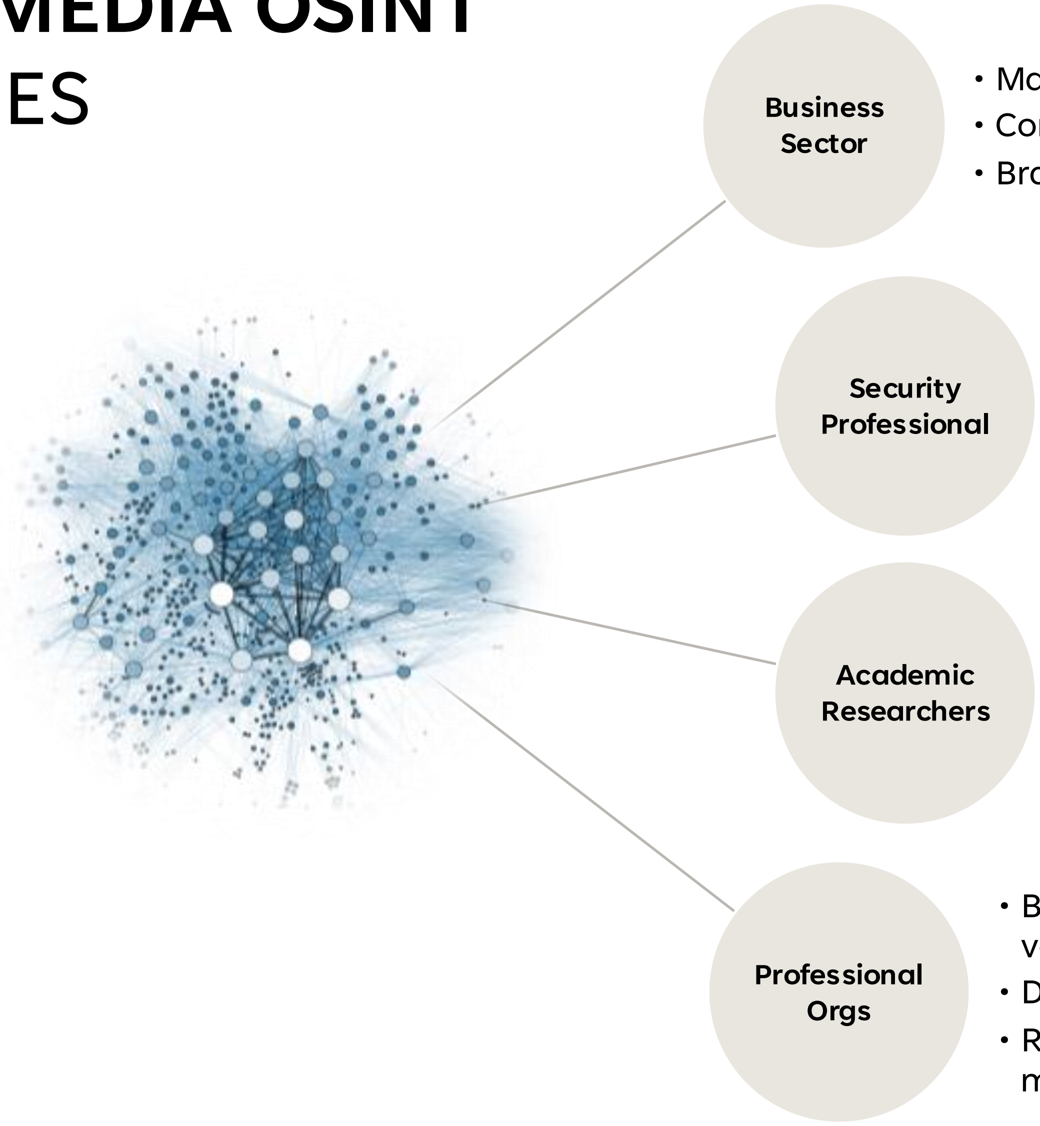
Gathering

- User profile scraping
- Tracking posting frequency for engagement patterns
- Geolocation data via public API
- Third-party social media monitoring platforms

Analysis

- Profile analysis (public content, engagement, networks)
- Cross-platform username analysis
- Temporal mapping of posting behaviors
- Network visualization
- Categorizing, pattern identification, and insight development

SOCIAL MEDIA OSINT
USE CASES



Business Sector

- Market research
- Competitor analysis
- Brand monitoring

Security Professional

- Threat assessment
- Fraud detection
- Event security planning

Academic Researchers

- Study social phenomena
- Conduct demographic research
- Analyze behavioral patterns

Professional Orgs

- Background verification
- Due diligence
- Reputation management

SOCIAL MEDIA OSINT ETHICS PRACTICING

We should be mindful of privacy rights, data protection regulations, and professional responsibilities.

- We should only collect and analyze publicly available information while respecting platform terms of service and user privacy settings.
- We must adhere to data protection laws, implement secure data handling procedures, and maintain transparent documentation of our methodologies.

OSINT USAGE IN WEBSITES AND BLOGS –REGINA

This can be broken down into three categories:

1)The first is OSINT that has been collected from a variety of sources and is being displayed as a news article to the public on a website. An example of this is Bellingcat.

2) The second is a collection of data from various sources which may or may not be open source but are collected by a website which is open source. An example is Tech Crunch.

3) The third is a website which does not mean to present data to the user that can help open source investigations but the collection of facts, email addresses, phone numbers, or images on it can be used as open source to discover information. Most other websites fall into this category

OSINT USAGE IN WEBSITES AND BLOGS –REGINA

Technique

The techniques for interacting with websites and blogs can range from simple research to using web scraping and archival webpage snapshots to see deleted materials. In relation to images on the website, these can be downloaded and if not properly scrubbed, the GPS coordinates ca n be salvaged from them, leading to a location.

Use cases

The use of these sources depends on what is being investigated. If you want to understand about VPNs and security vulnerabilities it may be useful to focus on niche blogs, collection of non open and open source information such as Tech Crunch or OSINT websites such as Authentic8.com
If you are trying to find out the location of an illegal political organization such as a Neo-Nazi group, scrapping their website for images to geo-locate or find incriminating details that were published and since been deleted are more useful.

Ethics

It is important to ensure that the data is fair and accurate. Malicious or misleading data can cause problems when repeated online. For example claiming that Indian Muslims are breaking down dams to declare water jihad.

Some information may violate the privacy of individuals and it is important to not “dox” them if there is no need.

It is important to follow laws regarding web scrapping and copyright when gathering data, particualrly from large databases.

ACADEMIC PUBLICATIONS OSINT – MPHO NKWANA

- Academic publications provide structured, factual, and specialized information encompassing various fields such as science, economics, and politics.
- Academic publications allow for data verification through references to prior studies, ensuring data credibility by cross-checking publications.
- OSINT analysts identify relevant databases and academic journals to gain insights from platforms such as PubMed and Google Scholar.
- Analysts then extract data and correlate the information with other OSINT sources such as social media and news reports to produce intelligence reports.
- Intelligence reports provide evidence-based results used for decision-making.

Google Scholar

PubMed.gov

ResearchGate

ACADEMIC PUBLICATIONS OSINT - TECHNIQUES

01

Using specific keywords in quotation marks to refine and filter searches and boolean operators such as AND and OR to control the scope of searches.

02

Investigating citations to pinpoint foundational research and cross-check findings across multiple sources by following the chain of citations.

03

Reviewing abstracts and metadata such as titles and authors to rapidly sift through sources and determine the relevance of publications.

04

Text mining tools for pattern recognition are used to extract relevant information such as numerical data and quotes from academic materials.

ACADEMIC PUBLICATIONS OSINT – USE CASES

Cybersecurity	Healthcare	Environment
• Used to understand emerging threats and best practices through foundational studies, historical data, and case studies • For example, a useful publication for analysts exploring ‘ransomware tactics’ includes articles in IEEE Transactions on Information Forensics and Security that contain information on attack patterns and ransomware detection methods.	• Provide insights into prevention measures and outbreaks which can be used to guide future responses to disease outbreaks • For example, medical journals like The Lancet published studies on vaccine efficacy and virus transmission during the COVID-19 pandemic that were used by governments and organizations to guide safety protocols and lockdowns.	• Used to develop and implement climate change policies and sustainable development processes. • For example, research published in *Nature Climate Change* on the impact of carbon emissions on global warming provides data for governments and organizations to support policies like carbon taxes.

ACADEMIC PUBLICATIONS OSINT – ETHICS

Academic publications often contain sensitive data and proprietary information, ethical guidelines prevent the misuse and ensure the integrity of information.

- Some academic publications are protected by copyright limiting the accessibility by enabling different levels of access. Access may require a subscription or a purchase and requires proper accreditation to prevent intellectual property infringement.

- Several academic publications contain sensitive data that may reveal information about participants and organizations and infringe on their privacy. The context of this data should be fully understood before it is used to gain insights, to eliminate bias and misinterpretation.

THANK YOU