OSINT in modern cybersecurity: weaponizing information

Angeliki Gioti
Offensive Security Consultant | Penetration Tester

regimes are using cyber-surveillance weapon to target journalists, human rights activists and politicians

Leak reveals global abuse of spyware by autocratic governments

Reporting team Stephanie Kirchgaessner in Washington, Paul Lewis, David Pegg, Sam Cutler and Dan Sabbagh in London, Nina Lakani in Mexico, Michael Safi in Beirut, Shaun Walker in Budapest, Angelique Chrisafis in Paris and Martin Hodgson in New York

Human rights activists, journalists and lawyers

was infected ject to an atte the consortiu indicative of NSO's governi in advance of attempts. Ana

OSINTde
@sentdef

At least 20 Paragliders were seen entering Northern Israel from Lebanon within the las few minutes.

10:35 AM · 10/11/23 from Earth · 746K V

1,615 Reposts 164 Quotes

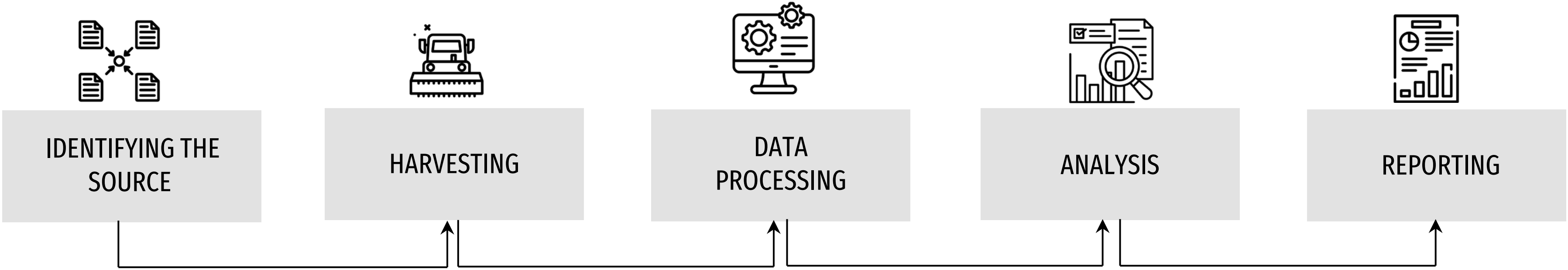
5,748

[Hood's comic Annual.

Indian Eloquence. A writer in the New-York Mirror, gives this lament of an Indian Warrior of the Yamassee tribe over the graves of his fathers and the recollections and affections of his youth. It is "the majesty of grief without its weakness."

OVERVIEW OF OPEN SOURCE INTELLIGENCE

OSINT revolves around information gathering and analysis from publicly accessible sources such as websites, social media platforms, news sources, academic publications, government reports, and public forum discussions.



OSINT is based only on the *passive* gathering of information. Value comes from analysis, pattern recognition and connecting the dots.

OVERVIEW OF OPEN SOURCE INTELLIGENCE

It can provide insights into various domains, from cybersecurity and national security to business intelligence and competitive analysis.

Cybersecurity & Cyberdefense	foot printing, forensics analysis, cyberattack attribution, social engineering, phishing attacks prevention.
Cybercrime & Organized Crime	identify illegal actions, retrieve suspicious traces, monitor malicious groups.
Social Opinion & Sentiment Analysis	marketing, political campaigns, disaster management, HR recruiting, journalism
Corporate Security	brand protection, fraud detection, insider risk monitoring
Everyday Use	background checks, personal safety, situational awareness, “stalking” your high school friends

CHALLENGES

Information Overload
The Web is a vast repository of information, manual work is overwhelming.

Need of Skilled Analysts
Effective OSINT Analysis requires skilled analysts for more efficient results.

Unstructured Data
The majority of data is unstructured, making it challenging to process and analyze.

OPEN SOURCES

the precise definition of “*Open Source*” is a subject that is open to debate. Sources like public records, personal SM accounts, and disclosed or leaked documents are considered “Open”. Documents labeled as “*Internal Use Only*” or “*Private/Confidential*” could potentially expose sensitive information, including patient data, passwords, or financial records, which are not intended for public disclosure. Social media platforms divulge extensive information regarding an individual’s identity, including potentially **overlooked data** stored within their personal profiles.

THE ROLE OF ARTIFICIAL INTELLIGENCE

INTEGRATION OF ARTIFICIAL INTELLIGENCE IN OPEN-SOURCE INTELLIGENCE

— automated data collection and aggregation

— techniques for processing and analyzing data

↳ NATURAL LANGUAGE PROCESSING (NLP), NAMED ENTITY RECOGNITION (NER), SPEECH TO FACE (S2F) etc.

— identification and classification of patterns and abnormalities

— predictive analytics and prospective projections

automated processes & tasks

improved accuracy & speed

scalability, accuracy, latency

data driven decision-making

Machine learning models can forecast cyber threats based on historical OSINT data.

Cross-platform correlation (Twitter, Telegram, Reddit, dark web) is possible in near real time.

Information is weaponized. OSINT can be used in detecting conflict initializations.

THE GRAY AREA

LOGISEK

Doxing

the malicious act of collecting and publicly disclosing **personal information** about an individual. The data may include the individual’s name, address, phone number, email address, social media profiles, and other *confidential* information. These practices are employed by malevolent individuals or collectives with malicious intentions, such as cyberbullies, hackers, and trolls.

Swatting

a criminal harassment act of deceiving an emergency service into sending a police or emergency service response team to another person's address. This is triggered by false reporting of a serious law enforcement **emergency**, such as a bomb threat, murder, hostage situation, or a false report of a mental health emergency.

[Vigilante justice to intimidate, manipulate, or humiliate a target in order to force them to comply.]

Hacktivism

employed as a means to gain social or political **benefits**; individuals may experience blemishes in their lives caused by reputational injury, job loss, and other undesirable consequences. In extreme cases, doxing can even lead to fatalities.

OSINT AS A TOOL IN MODERN (CYBER)WARFARE

— Expose vulnerabilities

↳ MAPPING CRITICAL INFRASTRUCTURE (POWER GRIDS, PIPELINES, TROOP MOVEMENTS) FROM OPEN SOURCES.

— Target individuals

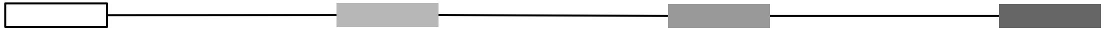
↳ DOXXING MILITARY PERSONNEL, JOURNALISTS, OR ACTIVISTS TO INTIMIDATE OR MANIPULATE THEM.

— Facilitate precision attacks

↳ COMBINING OSINT WITH CYBER TOOLS TO PLAN INTRUSIONS, PHISHING, OR INFLUENCE OPERATIONS.

Amplification	OSINT fuels narrative warfare.
False credibility	by citing "open sources," misinformation gains a veneer of legitimacy.
Destabilization	the goal often isn’t persuasion, but confusion.
Mass targeting	with OSINT-based profiling, propaganda can be micro-targeted.

OSINT AS A DOUBLE-EDGED SWORD



Cyber as the first strike

Cyber warfare

OSINT as a defensive detection tool

Early signs, sudden spikes

OSINT’s use in hacktivism

vigilantism vs. justice

Misinformation, propaganda

Influencing the public, loss of trust

ETHICAL CONSIDERATIONS & CHALLENGES

PRIVACY CONCERNS

— data collection & surveillance

(issues related to the protection of personal information and confidentiality)

— de-identification & anonymization

(necessary implementation of such protocols to ensure privacy protection)

BIAS AND FAIRNESS

— algorithmic bias

(addressing prejudice & guaranteeing fairness to avoid bias in training data)

— fairness

(avoid unequal effects, necessary for dependable decision-making)

SECURITY RISKS

— adversarial attacks

(safeguards against alterations of input data to ensure integrity of results
↳ protection against data breaches and illegal access.)

RELIABILITY AND ACCOUNTABILITY

— transparency

(openness, reasons should be justified & understandable)

— reliability

(absence of false positives & negatives to avoid inaccurate intelligence)

HUMAN FACTOR

(human supervision is essential to ensure that the process remains ethical)

COMPLIANCE WITH LAWS & REGULATIONS

(compliance to legal frameworks is **crucial**)

DUAL USE DILEMMA

(limit harmful applications. responsible development & monitoring)

Thank you for your time and attention.

Angeliki Gioti
Offensive Security Consultant | Penetration Tester
LOGISEK