THE 3RD REVOLUTION IN OSINT

Roy Zinman

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原“中国互联网安全大会”）

The Third Revolution in OSINT

OSINT and Cyber Security

OSINT - The 1st and 2nd Revolutions

The Challenges of OSINT

The Third Revolution

Case Study

OSINT & Cyber Security

OSINT (open source intelligence) - data that is collected from publicly accessible sources such as blogs, social media and discussion groups

OSINT is an essential component of cyber security

- Situational Awareness
- Risk Assessment
- Threat Detection
- Attack Surface Analysis

The Third Revolution in OSINT

OSINT and Cyber Security

OSINT - The 1st and 2nd Revolutions

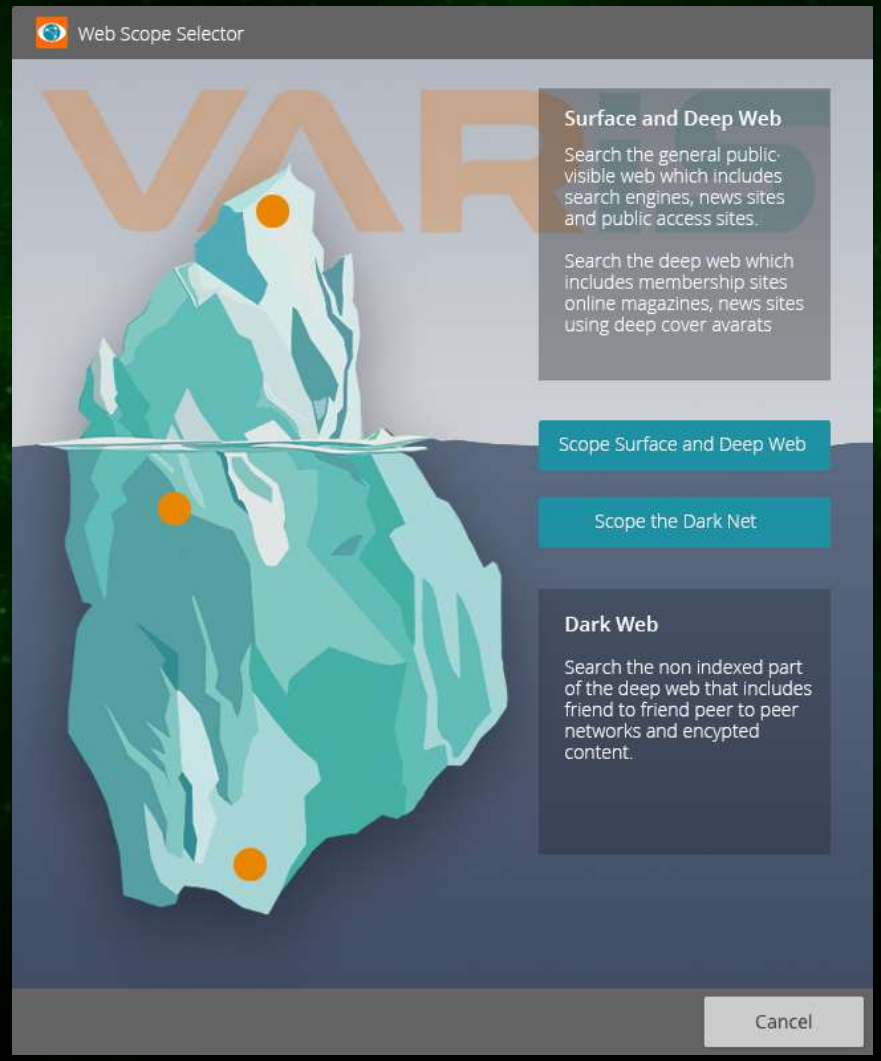
The Challenges of OSINT

The Third Revolution

Case Study

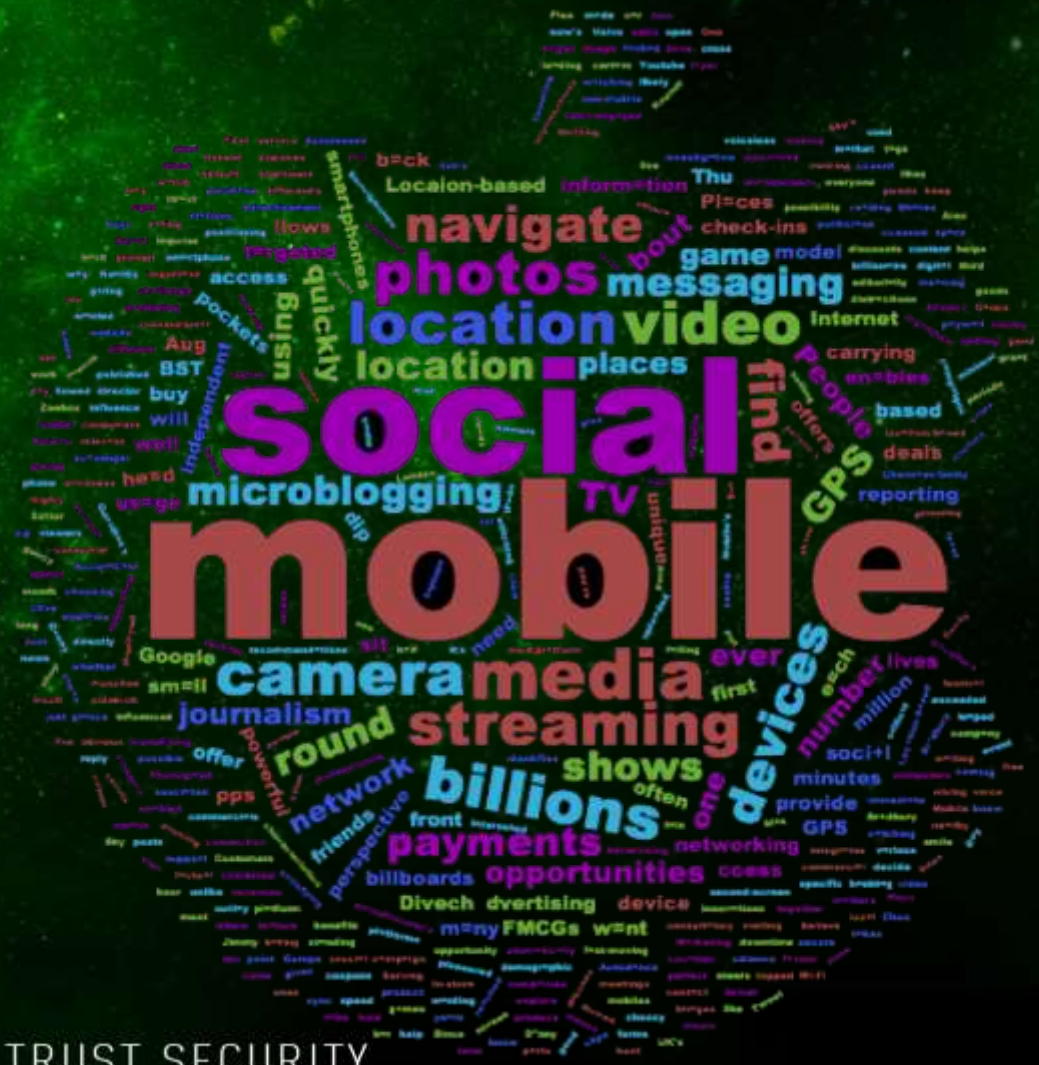
The First and Second Revolutions in OSINT

2005 - 2010 - The Social Media Revolution



The First and Second Revolutions in OSINT

2010 - 2015 - The Mobile Revolution



The Third Revolution in OSINT

OSINT and Cyber Security

OSINT - The 1st and 2nd Revolutions

The Challenges of OSINT

The Third Revolution

Case Study

The Challenges of OSINT

Real Time

Geo-tagged

Authentic

Diverse

Vast

Collect Mobile Information

Process Big Data

Privacy Protection

Validate Online Data

Understand Multiple Formats & Languages

Track Dynamic Sources

ZERO TRUST SECURITY

The Third Revolution in OSINT

OSINT and Cyber Security

OSINT - The 1st and 2nd Revolutions

The Challenges of OSINT

The Third Revolution

Case Study

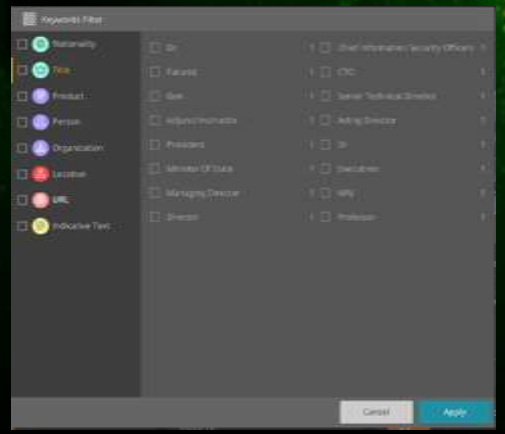
AI - The Third Revolution in Open Source Intelligence

Advancements in AI are rapidly transforming OSINT once again, and untapping a huge potential by:

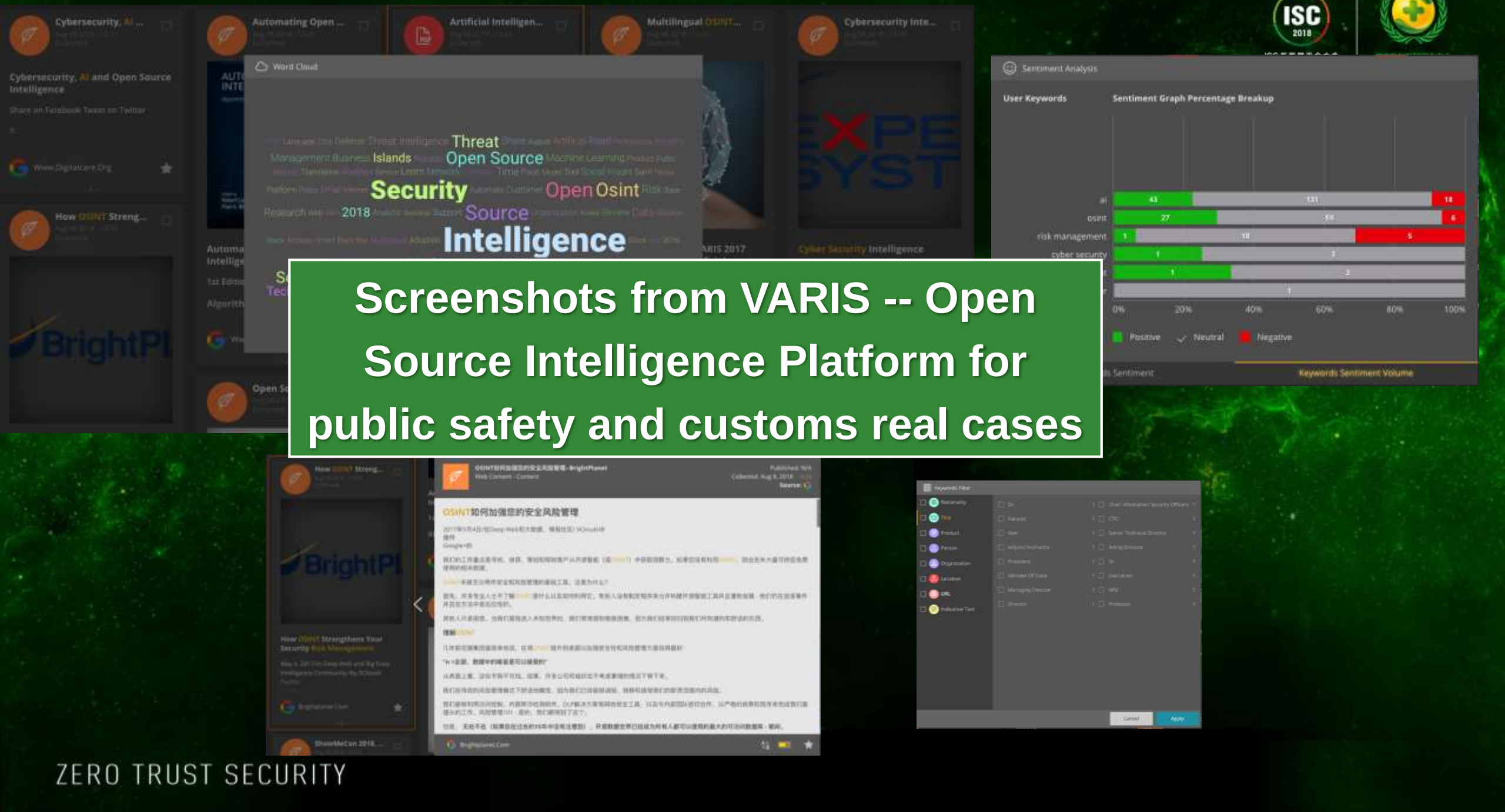
- Handling vast amounts of data by automated processing
- Automatically identifying risk patterns (unknown – unknown)
- Separating authentic and counterfeit data
- Using open source for predictive analysis
- Tackling privacy and commercial issues

AI Solutions Impacting OSINT

Machine Translation	Image Processing / Generation	Predictive Analytics	Natural Language Processing / Generation
Sentiment Analysis	Audio and Video Processing	Pattern Recognition	Connection Analysis



ZERO TRUST SECURITY


Word Cloud
Threat
Open Source
Islands
Security
Open Osint
2018
Source
Intelligence
Sentiment Analysis
User Keywords
Sentiment Graph Percentage Breakup
ai
osint
risk management
cyber security
0%
20%
40%
60%
80%
100%
Positive
Neutral
Negative
Keywords Sentiment Volume
Screenshots from VARIS -- Open Source Intelligence Platform for public safety and customs real cases
OSINT如何加强您的安全风险管理
ZERO TRUST SECURITY

The Third Revolution in OSINT

OSINT and Cyber Security

OSINT - The 1st and 2nd Revolutions

The Challenges of OSINT

The Third Revolution

Case Study

OSINT Importance For the Security of Israel

2020

2000

Threats are secretive, Intelligence is in closed systems

Threats are developing and culminating in cyberspace

ZERO TRUST SECURITY

OSINT Importance For the Security of Israel

Tracking the Development of ISIS

Cyber Threat Intelligence

The “Arab Spring” & Regional Stability

Boycott Movements

Monitoring the Situation in Neighboring Syria

ZERO TRUST SECURITY

Case Study - The “Lone Wolf” Wave of Attacks - 2015

- A wave of knife and ramming attacks starting in 2015 after an incitement campaign in Social Media (Facebook)
- Inciting content becomes viral, affects mainly teenagers
- Actors are unknown to the security forces of Israel
- Traditional intelligence gathering is useless
- Large amounts of data to process
- Low “Noise” ratio is a must
- High level linguistic capability is required

Case Study - The “Lone Wolf” Wave Attacks - 2015

Home > Israel News

Israel Thwarted Hundreds of Terror Attacks, Some With the Help of Big Data, Shin Bet Says

Israeli security service invested heavily in new technology, including machine learning and AI to thwart attacks 'even before they happen'

Josh Breiner | Jun 13, 2018 2:38 PM

81 Tweet 0 Zen

Around 250 terrorist attacks were thwarted in Israel this year and more than 400 Palestinians planning isolated attacks were arrested, Shin Bet security service head Nadav Argaman said on Wednesday.

HAARETZ

Summary

- OSINT has become an essential part of contemporary business and national security intelligence requirements, specifically cyber security
- The exponential growth in complexity and scale of data created numerous challenges for fulfilling OSINT potential
- AI advancements provide answers to many of the challenges in collecting and analyzing vast amount of data to create timely and actionable insights
- AI is going to transform both the way we create, share and consume data, and the way we create intelligence
- Harnessing advancements in AI to augment existing OSINT platforms and analysts will give an edge over competitors and adversaries


ISC
2018
ISC互联网安全大会
360互联网安全中心
THANKS
ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原“中国互联网安全大会”）