开源情报的第三次革命

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”）

开源情报的第三次革命

开源情报与网络安全

开源情报——第一次革命和第二次革命

开源情报的挑战

第三次革命

案例分析

开源情报与网络安全

开源情报（OSINT）是指从博客、社交媒体和讨论群组等公共信息来源中收集数据。
开源情报（OSINT）是网络安全的必要组成部分。

- 态势感知
- 风险评估
- 威胁检测
- 攻击面分析

开源情报的第三次革命

开源情报与网络安全

开源情报——第一次革命和第二次革命

开源情报的挑战

第三次革命

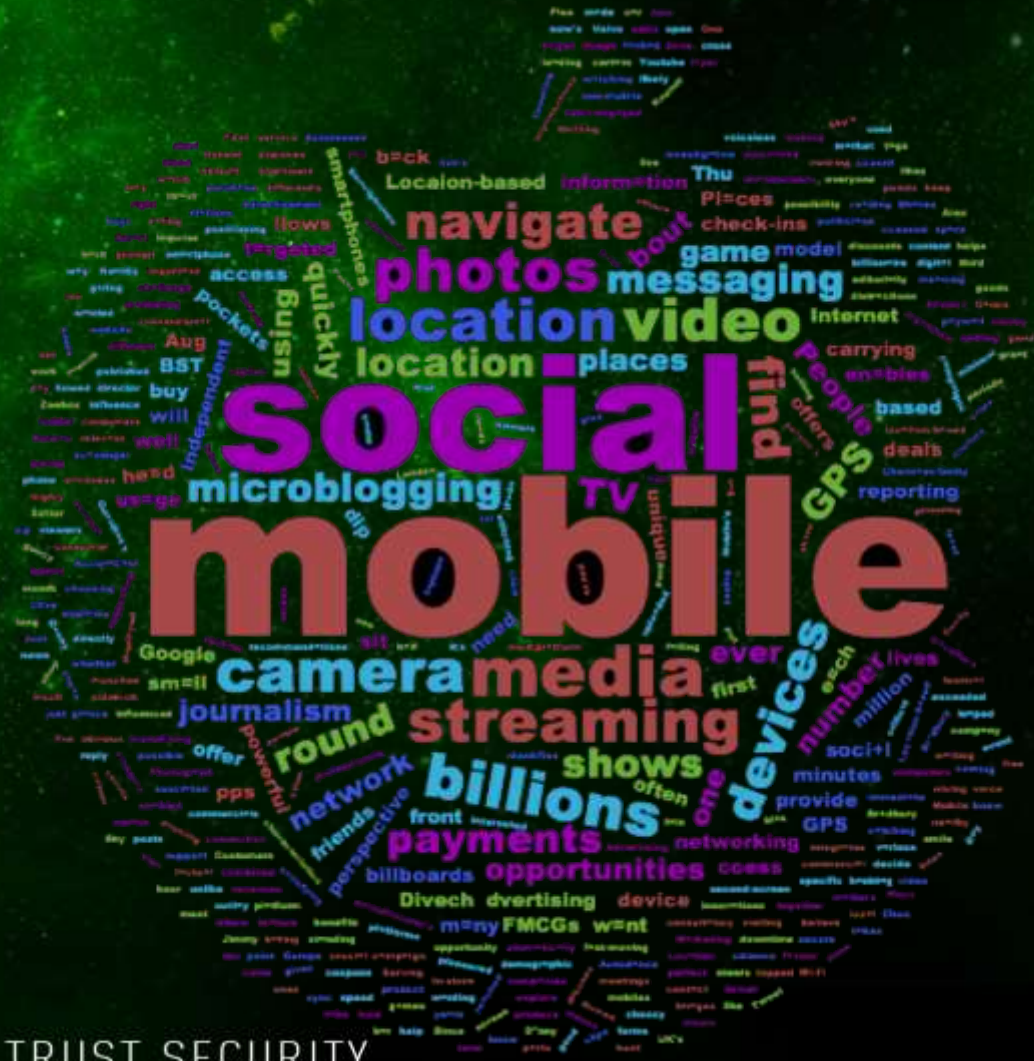
案例分析

开源情报的第一次革命和第二次革命

2005年 - 2010年——社交媒体革命

开源情报的第一次革命和第二次革命

2010年 - 2015年——移动技术革命



ZERO TRUST SECURITY

开源情报的第三次革命

开源情报与网络安全

开源情报——第一次革命和第二次革命

开源情报的挑战

第三次革命

案例分析

开源情报的挑战

实时

带有地理标签

真实可信

多元化

海量

收集移动设备信息

大数据处理

隐私 保护

验证在线数据

理解多种格式和语言

跟踪动态来源

ZERO TRUST SECURITY

开源情报的第三次革命

开源情报与网络安全

开源情报——第一次革命和第二次革命

开源情报的挑战

第三次革命

案例分析

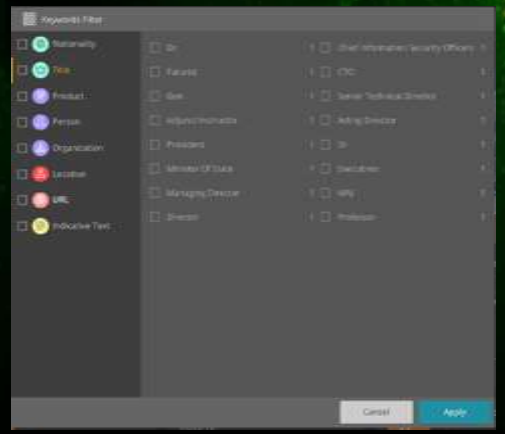
人工智能——开源情报的第三次革命

人工智能（AI）的进步正再次迅速改变开源情报（OSINT），通过以下方式发挥巨大的潜力：

- 通过自动化操作处理海量数据
- 自动识别风险模式（未知——未知）
- 分离真实和伪造数据
- 使用开放源码进行预测分析
- 处理隐私和商业问题

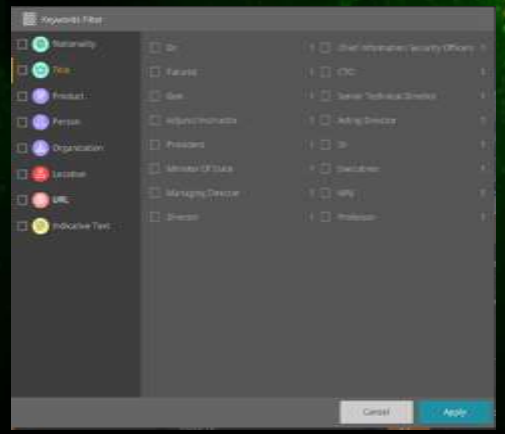
影响开源情报的人工智能解决方案

机器翻译	图像处理/生成	预测分析	自然语言处理/生成
情感分析	音频和视频处理	模式识别	连接分析



ZERO TRUST SECURITY

屏幕截图来自VARIS——应用于公共安全和海关真实案例的开源情报平台



ZERO TRUST SECURITY

开源情报的第三次革命

开源情报与网络安全

开源情报——第一次革命和第二次革命

开源情报的挑战

第三次革命

案例分析

开源情报对以色列安全的重要性

2000年

2020年

威胁具隐秘性，

情报相对闭塞

威胁在网络空

间发展蔓延并

达到顶峰

ZERO TRUST SECURITY

开源情报对以色列安全的重要性

追踪ISIS恐怖组织发展动态

网络威胁情报

“阿拉伯之春”与区域稳定性

抵制运动

监测邻国叙利亚局势

ZERO TRUST SECURITY

案例分析——2015年“独狼式”恐怖袭击狂潮

- 在社交媒体脸书网（Facebook）的煽动活动之后，2015年开始出现大量持刀、撞击式恐怖袭击
- 极具煽动性的信息像病毒般蔓延，主要对青少年群体产生影响
- 以色列的安全部队对于恐怖袭击者并不了解
- 传统情报收集无用武之地
- 需要处理海量数据
- 低信噪比的环境必不可少
- 需要高水平的语言能力

案例分析——2015年“独狼式”恐怖袭击狂潮

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

总结

- 开源情报（OSINT）已成为当代商业和国家安全智能要求的重要组成部分，特别是网络安全的重要组成部分；
- 数据复杂性及规模的急剧增长为实现开源情报（OSINT）潜能带来了许多挑战；
- 人工智能（AI）的进步为海量数据的收集和分析等众多挑战提供了及时、可操作的解决方案；
- 人工智能（AI）将改变我们创建数据、共享数据和使用数据的方式以及我们创建智能的方式；
- 通过人工智能（AI）进步来提升现有开源情报（OSINT）平台和分析师水平，将比竞争对手更具优势。


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”）