Clustering and information sharing

David Wright

Founder & Chief Research Officer

Trilateral Research

CEPOL European Research & Science Conference
“Preparing Law Enforcement for the Digital Age”
Vilnius, 8-10 June 2022

Today

- Rising cost of cybercrime
- AI will power cybercrime
- Cybercrime is greatly under-reported. What can we do about it?
- Clustering & other measures to connect LEAs & the private sector
- Invitation to join a WG to improve information sharing

TRILATERAL RESEARCH

First, a word about Trilateral Research

- Focus on ethical AI, platform services, data protection services, cyber security and research
- Wide range of clients from governments, universities, healthcare providers, international organisations
- Offices in London and Waterford, Ireland
- 120 people, majority with post-doctoral experience
- Partnered in more than 70 EU-funded projects since 2004
- trilateralresearch.com

TRILATERAL RESEARCH


TRACE
PROTAX
H2020
PIAF
PRIVACY IMPACT
ASSESSMENT FRAMEWORK
IRISS
INCREASING RESILIENCE
IN SURVEILLANCE SOCIETIES
DARLENE
Deep AR Law Enforcement Ecosystem
DANTE
EUNOMIA
IRISS
INCREASING RESILIENCE
IN SURVEILLANCE SOCIETIES
INSPECTr
COPKIT
SHERPA
SAPIENT
Surveillance, Privacy & Ethics
byte
ETTIS
INSPEC²T
sienna.
PRISMS
PHAEDRA
IMPROVING PRACTICAL
AND HELPFUL COOPERATION
BETWEEN DATA
PROTECTION AUTHORITIES
CRISP
Evaluation and Certification
Schemes for Security Products
CC-DRIVER
PRIPARE
PReparing Industry to Privacy-by-design by supporting its Application in REsearch
ROXANNE
CYBERSPACE
FORTRESS
Foresight Tools for
Responding to
cascading effects
in a crisis
TRACE
TRafficking as A Criminal Enterprise
PREVISION
TRILATERAL
RESEARCH

The rising cost of cybercrime

- Cybercrime has become entrenched in our society

  [Europol]
- More than half of all cyberattacks are committed against small-to-mid-sized businesses [Europol]
- The likelihood of detection and prosecution is as low as 0.05% in the United States [WEF Global Risk Report, 2020]
- The frequency and complexity of ransomware attacks increased by more than 150 per cent in 2020 [JRC]

TRILATERAL RESEARCH

Ransomware attacks double in a year

- Healthcare organisations saw ransomware attacks almost double between 2020 and 2021, according to a survey released last week by Sophos.
- Healthcare orgs are likely to pay ransoms
- But they rarely get all of their data back.
- 78 per cent of organizations sign up for cyber insurance to reduce their financial risks
- 97 per cent of the time the insurance company paid some or all of the ransomware-related costs.

TRILATERAL RESEARCH

What is the cost of cybercrime?

- CSIS and McAfee report (2018) concluded that close to $600 billion, nearly one per cent of global GDP, is lost to cybercrime each year
- "Into the Web of Profit" project made a conservative estimate of $1.5 trillion of the annual global revenues derived from cybercrime (Dr. Mike McGuire, 2018).
- Cybersecurity Ventures estimated $5.5 trillion in 2020.
- The annual cost of cybercrime to the global economy in 2020 is estimated to be €5.5 trillion, double that of 2015-16. This represents the largest transfer of economic wealth in history (EU Cybersecurity Strategy, Dec 2020)

TRILATERAL RESEARCH

Cybercrime affects everyone

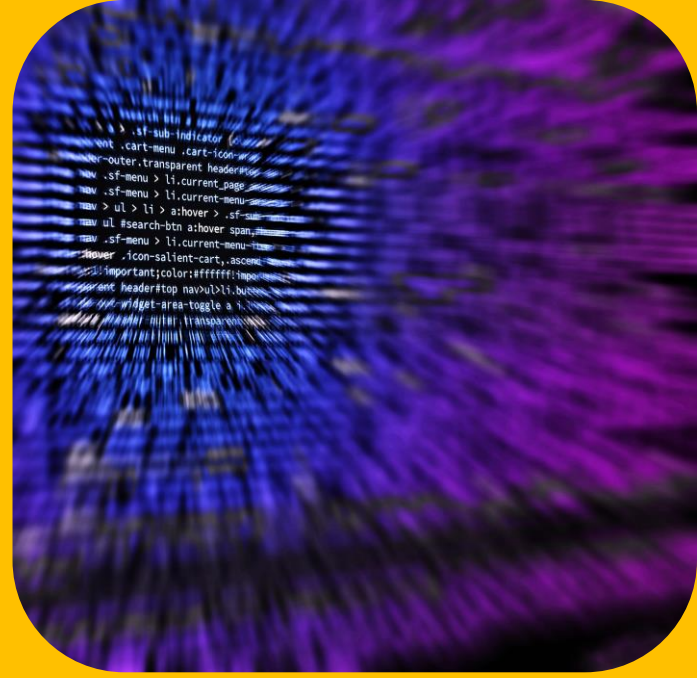
- As ICT becomes more embedded in our society and cyber-physical systems ubiquitous, cybercrime has become a common hazard on a global scale. With more than *4.5 billion people online*, *half of the world's population is at risk* of falling victim to cybercrime [Interpol, NCS 2021].
- Nearly two-fifth of users (circa 2.7 billion) have experienced security-related problems and more than half feel unable to protect themselves against cybercrime [EC Cybersecurity Strategy, 2020].
- Subsequent cyber-offences – e.g., online identity theft, financial fraud, extortion and sale of proprietary and sensitive information on dark web markets – pose an increasing and potentially never-ending risk of victimisation.

TRILATERAL RESEARCH

Socio-economic impact of cybercrime

- Measuring the impact of cybercrime enables the criminal justice system to shape effective policies and operational responses. It allows evidence-based mobilisation and alignment of resources [Glacy+ 2020].
- The impacts of cybercrime may trigger chain reactions throughout the economy and societal levels (e.g., crypto-ransomware attacks and attacks against critical infrastructure sectors).
- The EU, Member States and LEAs face resource constraints to address the different types of cyberattacks that confront enterprises of all sizes.

AI will power cyberattacks & cybercrimes



- AI hasn't been used much yet in cybercrime, but its use is growing and experts have warned that it will transform cybercrime
- AI is likely to ratchet up the effectiveness and impact of cybercrimes, including cyber attacks.
- We are only at the beginning of the widespread use of AI-based systems [JRC] e.g., via autonomous social engineering, social media manipulation, and AI-based fake content
- "AI is deepening the threat posed by cyber attacks and disinformation campaigns that … state and non-state actors are using to infiltrate our society, steal our data, and interfere in our democracy. The limited uses of AI-enabled attacks to date are the tip of the iceberg" [NSCAI]

TRILATERAL RESEARCH

AI & cybercrime

- AI is used to generate deepfakes for pornography, fraud, extortion, phishing
- AI can be used to target individuals based on their social media activity
- Disinformation
- Malware
- Harassment and defamation
- ML poisoning attacks – AI is used to poison the data and models used in AI-based systems, incl. cybersecurity defences

TRILATERAL RESEARCH

Malware & machine learning

- Malware developers can use AI in more obfuscated ways without being detected by researchers and analysts.

Malicious Uses and Abuses of Artificial Intelligence

Report by Trend Micro Research, United Nations Interregional Crime and Justice Research Institute (UNICRI), Europol's European Cybercrime Centre (EC3), 2020

TRILATERAL RESEARCH

A warning from the NSCAI

TRILATERAL RESEARCH

- Malware in the AI era will mutate into thousands of different forms once it is lodged on a computer system
- AI makes it harder for anyone to hide his or her financial situation, patterns of daily life, relationships, health and even emotions
- Personal and commercial vulnerabilities become national security weaknesses as adversaries map individuals, networks, social fissures and how best to manipulate behaviour and cause harm

Under-reporting

- Experts, EC, LEAs believe cybercrime is significantly under-reported
- Cybercrime remains widely under-reported [ISACA]
- FBI believes fewer than 12% are reported [Slate]
- Fewer than 2% of cybercrimes are reported [UK Office for National Statistics]

TRILATERAL RESEARCH

Reasons for not sharing information

- Reputation damage
- Fear of impact on share price
- Legal ambiguity
- Risk aversion
- Limited resources
- Lack of awareness – What is a cybercrime? Who to report to?
- Belief that LEAs can't or won't be able to do anything about it because they don't have the resources or [AI] competencies

TRILATERAL RESEARCH

Reasons *for* sharing information

- Help give us a better picture of the scale of cybercrime and cyberattacks. No one knows the true scale of cybercrime.
- With a better understanding of the true scale of cybercrime, politicians and decision-makers are more likely to allocate appropriate resources. If only one company reports a cyberattack, politicos are likely to ignore it. If 100 report attacks, they are less likely to do so.
- Sharing information gives us a better understanding of the cybercriminals and cyberattackers, of the tricks they use, of their targets and malware.
- It's in the financial and economic interest of all companies to combat cybercrime.
- Withholding information – not sharing it – makes it harder to combat cybercriminals.

TRILATERAL RESEARCH®

Connecting with stakeholders

- Cybersecurity Act of 2019 refers to ENISA's role in stimulating cooperation and information-sharing between and with the public and private sectors and within the private sector.
- The EC Cybersecurity Strategy says a "global, open, stable and secure cyberspace" requires "regular and structured exchanges with stakeholders, including the private sector, academia and civil society".
- NIS 2 directive obliges "essential and important" entities to report significant threats and incidents to the competent authorities or the CSIRT within 24 hours after having become aware of the incident and a detailed report not more than one month later.
- EC also funds projects.

TRILATERAL RESEARCH

Initiatives to improve reporting & cooperation:
CC-DRIVER

Examining human and technical drivers of cybercrime	Developing AI-assisted tools for threat research and incident investigation	Consortium includes five LEAs plus companies and universities	CC-DRIVER has a Stakeholder Board, including 6 LEAs
We consult an EAB & SAB	LEA working group led by PLV	LEA project cluster	Webinars, interviews

TRILATERAL RESEARCH

LEA project cluster

- Started with eight projects, now 18 in the cluster
- Projects all have LEAs in their consortia and stakeholder boards
- Shared objectives
- Coordinators meet quarterly
- Cluster is a way of leveraging impact
- Joint response to the EC consultation on proposed Cyber Resilience Act
- Sharing thoughts on common challenges (getting access to real data, generating impact, turning results into things that LEAs can actually use, etc)

TRILATERAL RESEARCH

Clusters with and without the EC

- LEA cluster comprises only projects, their coordinators & partners
- LEA Working Group prefers just LEAs, no third parties, to facilitate free, open and unattributed discussion (but each mtg produces a summary report)
- EC is taking a steering role in a new Climate change and Health Cluster", comprising six projects resulting from an EC call. DG RTD "will act as the overall supervisor ensuring the smooth running of the cluster"

TRILATERAL RESEARCH

Other cluster differences

- EC cluster has a fixed term, to end 2026
- EC cluster has prescribed activities
- EC cluster has shared communications activities, e.g., a cluster brochure, a cluster newsletter, annual meetings, a cluster portal, stakeholder list
- Cluster working groups
- A cluster advisory board
- Rotating leadership
- Mandatory joint deliverables, periodic joint reports
- Cluster costs come out of project budgets

TRILATERAL RESEARCH®

Cluster guard rails

- Cluster shelf life
- Finances (organising meetings takes time)
- Limits to the size of the cluster
- Facilitation (even co-design requires specialised skills)

TRILATERAL RESEARCH

Initiatives to improve reporting & cooperation: CYBERSPACE

Consortium includes LEAs and companies

ISF, ECSO, INTERPOL have agreed to be on the Stakeholder Board

Questionnaires on reporting cyberattacks

Formation of a working group of LEAs for sharing information and collaboration on cybercrimes

Formation of a working group of private sector participants on reporting cyber attacks and cybercrimes

Formation of an industry-LEA working group

TRILATERAL RESEARCH

Information sharing: current challenges

- Important to better understand and identify attackers
- Governments take initiatives to share information on a national or societal level, but feedback, responses on an individual case level is lacking
- Real or perceived barriers to data sharing and retention, placed by the GDPR and the Law Enforcement Directive 2016/680
- We need collaboration – a working group - between industry & LEAs in CYBERSPACE
- Focus of WG is on info sharing – to get a better understanding of the extent of cybercrime and what can be done to improve reporting
- Information sharing has to be two way

TRILATERAL RESEARCH

Please

- You are invited to join a CYBERSPACE working group to see what can be done to improve reporting, to get a better measure of the true extent of cybercrime, to provide feedback to victims and to discuss active defence measures that companies can take to repel attacks.
- Active defence issues need discussion among LEAs, industry, SMEs, policymakers and academics
- LEAs should take an active part in defining their AI technology expectations and the tools they hope to get from projects
- To reduce cybercrime, everyone needs to cooperate and share information

TRILATERAL RESEARCH®

Thank you for your attention

Contact us:

david.wright@trilateralresearch.com [CC-DRIVER]

nikola.tomic@trilateralresearch.com [CYBERSPACE]

www.trilateralresearch.com
https://www.ccdriver-h2020.com
http://cyberspaceproject.eu

CC-DRIVER received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543. CYBERSPACE has received funding under the EU's Internal Security Fund — Police (ISFP) programme under grant agreement No 101038738.