INTRODUCTION TO MEDI@4SEC

CoU Event, 6 December 2017
Brussels, Belgium

Co-funded by the Horizon
2020 Framework Programme
of the European Union

INTRODUCTION

- **Ethical/Societal Dimension Topic 3: Better understanding the role of new social media networks and their use for public security purposes**

MEDI@4SEC will create a future vision for the role of social media in law enforcement and public security planning, not only for communication purposes and as a listening platform, but also as a collaboration platform – a digital realm where policing and crime prevention can be done in new ways with new types of (digital and real world) interventions.

The evolution being brought about by social media has tremendous implications for organisational transformation, but also for society as it prompts re-evaluation of ethical principles and legal and data protection protocols.

Co-funded by the Horizon
2020 Framework Programme
of the European Union

MEDI@4SEC AIMS

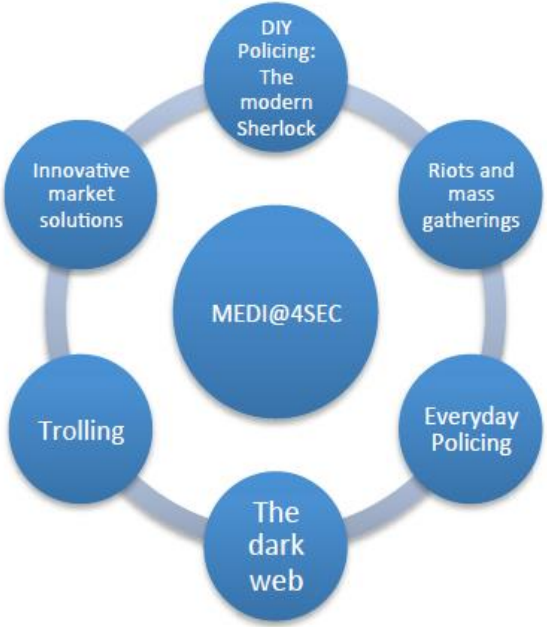
MEDI@4SEC digs into the good, the bad and the ugly of social media use in enhancing public security

Q1: How and why are new forms of social media currently being adopted and used by public security planners, citizens and criminals?

Q2: How should social media use amongst law enforcement, public security planners and citizens evolve in the future and influence operational practices and requirements?

Q3: What are the social, ethical and legal implications of this increased use of new social media?

One of the main conclusions of this analysis it that the whole dark markets ecosystem revolving around the business value chain acquires a potential responsibility in reducing crime. This includes private sector actors such as fintech and financial services, logistics providers, internet services providers, and citizens at large.


DIY Policing: The modern Sherlock
Riots and mass gatherings
Everyday Policing
The dark web
Trolling
Innovative market solutions
MEDI@4SEC

Co-funded by the Horizon 2020 Framework Programme of the European Union

Policing the Dark Web

Outcome of MEDI@4SEC workshop, Den Hague, 27 September 2017

Serena Oggero, Mark van Staalduinen, Marijn Rijken

TNO innovation for life

WORKSHOP APPROACH

- A one day international workshop with
  - 65 participants actively involved in fighting crime on the dark web: law enforcement organisations, governments, international institutions, and research and technology experts
  - 10 short key note presentations to set the scene and share good practices
  - 20 small focus group dialogues to identify opportunities
  - 1 closing panel to formulate actions

Co-funded by the Horizon
2020 Framework Programme
of the European Union

POLICING THE DARK WEB: CENTRAL QUESTION

- The central question is:

  How to reduce (eliminate) criminal behaviour on the Dark Web?

- Approach: start from the business model of criminals on the Dark Web.

- Underlying questions are:

  Is it a buyer's or a seller's market?

  What is the incentive or motif driving the market?

  And how can we eliminate it to disrupt the business model?

STRUCTURE BY TYPE OF “PRODUCT”

DRUGS (~80%)

- The main motif is to make as much money as possible.
- It is a seller-driven market.

- How to disrupt the business model? Make sure there is no more money to gain in this way *(e.g., make sure sellers are not trusted anymore, or that technically transactions become unstable and money is lost, etc)*

The strategy is clear. Need: re-inforce, structurally apply

TERRORISM-RELATED PRODUCTS

- The main motif is to perpetuate terrorist actions.
- It is a buyer-driven market.

- How to disrupt the business model? Make sure the buyer feels at risk *(e.g., de-anonimize buyer)* or reduce the demand *(e.g., de-radicalisations strategies).*

The strategy is not clear yet. Need: develop.

CYBERCRIME SERVICES

- The main motif might be hybrid warfare.
- It is both a seller-driven and buyer-driven market.

The stake and goal itself are not clear yet! Need: understand.

DISCUSSION QUESTIONS

- 1) International operation: What needs to be in place to conduct a successful **international operation** (on the criminal trade of product X)?
  - Example expected answer: collect and share so much information on the ecosystem and business model that it can be understood and brought to a hold

- 2) National / regional identification: Let's assume that the international operation is successful and lead to local leads. What needs to be in place (at the level of national and regional actors) to be able to conduct a successful **local identification operation**?
  - Example expected answer: the link between international and local organisations should be good and working to share intel, the region should be prepared to act

- 3) From Prosecution to Court: Let's assume that the local identification operation is successful and lead to an identified suspect. What should be in place to be successful at every step of the prosecution of the identified suspect?

MAIN MESSAGES

Crime on the dark web is a **global digital problem**. We need a new approach to intelligence to achieve Situation Awareness in this context.

RECOMMENDED ACTIONS

- **Common repository** in place and browsable by all (at least European) LEAs.
- To store not only criminal data and information from investigations, but also investigation practices, tools and methods, current focus of operations, criminal behaviours and patterns, contacts of investigation and prosecution experts.
- Necessary to leverage coordination between countries and units and **reduce double efforts**.

MAIN MESSAGES

In the last year, we registered the **first global policing successes**, one example being the take down of AlphaBay and Hansa. What lessons do we learn?

RECOMMENDED ACTIONS

- Europol and Interpol to play a role in centrally coordinating operations and stimulating a collaborative sharing culture.
- Investigation approaches to **break the traditional policing 'silo's'.**
- Criminals mistakes to be detected and exploited.
- Methods to link the digital and physical patterns of users.

MAIN MESSAGES

We deal with a large international ecosystem, whose **technologies** –such as cryptocurrencies, **are world-wide and not illegally deployed**. Governmental agencies do not have enough resources to act, but private businesses do.

RECOMMENDED ACTIONS

- Public-private collaborations to be simulated, as well as team work between LEA and knowledge organisations.
- **Private sectors (e.g., Internet service providers) to be stimulated to collaborate** not only passively, by sharing information when needed, but mostly **proactively by deploying resources and taking responsibility.**

RESULTS & OUTLOOK

- A successful workshop! Why?
  - Experts from different ‘silo’s’ could meet, share and work together
  - A common global picture, new underlying connection lines are born

- Insights on various dimensions
  - Governance, operational, technological, ethical..

- Report available on our website http://media4sec.eu/downloads/d2-5.pdf

- Next workshops:
  - Trolling, May 2018
  - Innovative market solutions, September 2018