CYCLOPES

CYBERCRIME LAW ENFORCEMENT PRACTITIONERS NETWORK

CYCLOPES - Fighting Cybercrime – Law Enforcement Practitioners' Network

Deliverable D4.8

2nd Annual innovation uptake recommendations

Public

This project has received funding from the European Union's Horizon 2020 - the Framework Programme for Coordination and Support Action (2014-2020) under grant agreement No. 101021669

DOCUMENT INFORMATION

Deliverable reference number	D4.8
Deliverable name	2nd Annual innovation uptake recommendations
Deliverable type	Report
Dissemination level	Public
Work package contributing to the deliverable	WP4
Due date	30/04/2023
Version	1.0
Actual submission date	02/06/2023

Responsible organisation	IANUS
Editor(s)	Dimitris Kyriakou, Georgios Georgiou
Contributor(s)	PPBW
Reviewers(s)	Rashel Talukder

Disclaimer	This document reflects only the view of its authors, and the European Commission is not responsible for any use that may be made of the information it contains.

DOCUMENT CHANGE CONTROL

Version	Date	Status	Author(s), reviewer	Description
0.1	15/06/2022	Draft	Dimitris Kyriakou, Georgios Georgiou	Initial Draft, TOC
0.2	30/10/2022	Draft	Dimitris Kyriakou, Georgios Georgiou	Editing Sections 3,4,5
0.3	13/03/2023	Draft	Dimitris Kyriakou, Georgios Georgiou, Georgios Kioumourtzis	Editing Sections 6 completion of interview
0.4	13/04/2023	Draft	Dimitris Kyriakou, Georgios Georgiou, Georgios Kioumourtzis	Final draft for internal review
1.0	02/06/2023	Final	Rashel Talukder	Final approval and submission

Table of Contents

1. Summary

The CYCLOPES project intends to create and preserve an innovation-driven network of Law Enforcement Agencies (LEAs) battling cybercrime, enhancing the EU's capabilities to combat growing cyber threats. With innovation at the core of LEA's operations, a new discussion begins regarding how all this innovation will be managed. Innovation uptake expresses that process and consists of four major concepts: identifying the specific needs of users, using the best innovative procurement model for the job, ensuring the greatest impact of a new innovation and finally, validation of the innovation. In this document, existing frameworks, best practices and other related activities are gathered in an attempt to guide this process of Innovation Uptake. This is the first report of five that will be updated as the project progresses.

The current document aims to provide recommendations for law enforcement agencies (LEAs) involved in combating cybercrime on how to acquire and implement new tools or methodologies in their everyday work. The use of advanced technology in fighting cybercrime is becoming increasingly essential, and it is crucial for LEAs to stay updated with the latest tools and techniques.

One of the most popular and widely used tools in the market for digital forensics and mobile device analysis is Cellebrite[1]. Cellebrite provides a range of tools and solutions that help LEAs in acquiring, analysing, and reporting digital data from various devices. However, it is essential to note that the term "new tool" used in this document refers to any tool or technology that is new to the particular LEA department.

Acquiring a new tool or technology can be a complicated process, and it is crucial to have a well-defined plan to ensure a smooth transition and successful implementation. LEAs should first conduct a thorough analysis of their current processes and identify the gaps or areas where a new tool or technology could be beneficial. They should then research and evaluate various tools and technologies available in the market, considering factors such as compatibility, cost, ease of use, and effectiveness[2].

Once a suitable tool or technology has been identified, LEAs should develop a plan for implementation and training. The plan should include steps for installation, configuration, data migration, and testing. Additionally, LEAs should ensure that their staff is adequately trained on how to use the new tool or technology effectively.

It is also essential for LEAs to keep up with the latest developments and advancements in the field of cybercrime and digital forensics. They should attend conferences and training programs to stay updated on the latest tools and techniques.

In conclusion, acquiring and implementing a new tool or technology can be challenging, but with proper planning, research, and training, LEAs can successfully adopt new tools and techniques in their everyday work.

[1] Cellebrite. (n.d.). Digital Intelligence Solutions. Retrieved from https://www.cellebrite.com/en/home/

[2] Casey, E. (2018). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press.

2. Introduction

Innovation is a crucial driver of economic growth and development. It refers to the creation of new or improved products, services, or processes that are different from previous ones and are made available to potential users or brought into use by the unit. Innovation can take different forms, such as incremental improvements, radical innovations, or disruptive innovations.

Innovation plays a crucial role in improving living standards by creating new jobs, increasing productivity, and enhancing competitiveness. It is a key driver of economic growth and helps to create new opportunities for businesses, individuals, and countries. In fact, countries that are more innovative tend to have higher levels of economic growth, income, and overall well-being[3].

Innovation is typically based on knowledge-based activities that involve the practical application of existing or newly developed information and knowledge. Information consists of organized data that can be easily reproduced and transferred across organizations at a low cost. Knowledge, on the other hand, refers to the understanding of information and the ability to use it for different purposes. Knowledge is typically acquired through cognitive effort, and it can be difficult to transfer because it requires learning on the part of the recipient.

Innovation can be sourced or created within or outside an organization. Internal innovation involves developing new products, services, or processes within an organization. External innovation, on the other hand, involves sourcing ideas, technologies, or expertise from external sources, such as research institutions, universities, or other firms.

In conclusion, innovation is a vital driver of economic growth and development. It involves the creation of new or improved products, services, or processes that differ significantly from previous ones. Innovation is typically based on knowledge-based activities that involve the practical application of existing or newly developed information and knowledge. Both information and knowledge can be sourced or created within or outside an organization, and they play a crucial role in the innovation process.

The consortium of CYCLOPES - Fighting Cybercrime – Law Enforcement Practitioners' Network is evaluating how innovative Cybercrime-fighting tools or methods can be taken up by LEAs (Law Enforcement Agencies).

[3] Organization for Economic Co-operation and Development (OECD). (2015). Innovation, productivity and growth. Retrieved from https://www.oecd.org/sti/inno/Innovation-Productivity-and-Growth-2015.pdf

Terms

- **Innovative tool or innovative method:** For the purpose of this survey, we define innovative, any tool or method that you consider new for your agency. In other words, innovative is a tool or method against Cybercrime that is not well-established yet in your agency.
- **Uptake:** Is defined as the process of integrating a new innovative tool or method to your standardized everyday processes for fighting Cybercrime.
- **Cybercrimes** can be a non-exhausting list of crimes as for examples crimes that can be committed using the internet (such as hacking for industrial espionage); or are enabled by the internet (such as fraud); or crimes where there is a digital evidence opportunity (e.g., burglary where the suspect inadvertently leaves their mobile phone details on a router) or any other crime your agency considers as cybercrime.

Examples of innovative solutions:

1. Cellebrite premium – get access to mobile phones – passcode

Brief description:

Cellebrite Premium is a comprehensive on-premise solution that **empowers your law enforcement agency to access iOS and high-end Android devices**. Cellebrite Premium grants you unparalleled access to digital evidence found in highly-protected areas like the Secure Folder and iOS Keychain.

Useful links:

- https://cellebrite.com/en/home
- Cellebrite - Digital Intelligence For A Safer World

2. Centralized system license

Brief description:

Dongle server (administrator gives access to different categories for LEA employees). The dongle server works like a virtual cable extension over the network, which you use to control the dongles and use them just as if they were connected locally.

Useful link:

- https://www.seh-technology.com/us/products/usb-dongle-servers.html

3. Black box Internet traffic monitoring – track attacks / risks

Useful links:

- https://www.alertlogic.com/blog/how-network-traffic-can-mask-a-serious-cyber-threat/
- https://www.sentinelone.com/blog/black-box-monitoring-track-opaque-systems/

4. Phishing-websites early detection

Brief description:

This can be done by first monitoring the (publicly available) stream of new SSL certificates being registered and filtering out domains which could indicate phishing. These could be variations on names of common banks and government institutions. Based on several indicators, a short list of potential phishing websites can be automatically compiled.
Each of these websites on the short list will then be monitored for several days to see if it contains unique elements of known phishing kits.
When this is detected, we can assume this webpage is being setup for use as a phishing page and further steps can be undertaken to take down the page and identify the creator(s) of the website.

Useful links:

- https://www.nature.com/articles/s41598-022-10841-5
- https://www.peertechzpublications.com/articles/TCSIT-6-140.pdf
- https://link.springer.com/article/10.1007/s42979-022-01069-1

5. Digital Forensics (DF)

Brief description:

Digital forensics in general is closely related to Cybercrime since it is used to analyse (potentially) compromised devices for traces of malware, indicators to who the perpetrators might be, evidence on a suspects pc, etc.
DF is broader then cybercrime though and is used in all sorts of judicial investigations. It is also one of the recurring 'general' themes in the CYCLOPES workshops.

Useful links:

Automation of forensic procedures (child abuse):

- https://www.sciencedirect.com/science/article/pii/S1742287619301549

Digital vans / mobile forensics labs:

This link relates to crime scene digital forensics the ability to triage at scene to limit the seizure of devices back to the laboratory thereby allowing victims and witnesses to have access to their devices as quickly as possible.

- Mobile forensics - Complete solution from MSAB

3. Defining Innovation

3.1. Main Innovation Activities

The main eight types of activities that organizations undertake in pursuit of innovation are displayed below while many of these mostly knowledge-based activities can also be used for other, more general goals.

Research and experimental development activities
R&D is a methodical and imaginative process that seeks to enhance knowledge and explore new applications for it. Applied research has a particular practical objective or target, while experimental development aims to generate new products or processes or enhance existing ones. This leads to a drive for innovation.

Engineering, design, and other creative work activities
Engineering, design, and other creative work involve experimental and imaginative tasks that are associated with R&D but may not meet all five R&D criteria. These tasks can consist of follow-up or auxiliary R&D activities, as well as independent activities that are not part of R&D.

Marketing and brand equity activities
Marketing and brand equity activities involve market research, market testing, pricing, product placement, promotion, advertising, trade shows, and the development of marketing strategies, as well as public relations efforts that enhance a company's reputation and brand equity. These activities do not encompass sales and distribution.

Intellectual property-related activities
IP-related activities involve protecting and commercializing knowledge developed through R&D, software development, engineering, design, and other creative activities. This includes administrative and legal work to apply for, manage, trade, license-out, market, and enforce a firm's intellectual property rights (IPRs) such as patents, trademarks, copyrights, and trade secrets.

Employee training activities
Employee training includes any company-sponsored or subsidized activities that equip employees with the knowledge and skills necessary for their occupation, profession, or job. Examples of employee training include on-the-job training and job-related education at educational institutions.

Software development and database activities
The development of software to create new or improved business processes or products, such as computer games, logistical systems, or software to integrate corporate operations, is considered an innovation activity. Database operations are also considered an innovation activity when they are utilized for innovation purposes, such as analysing data on material qualities or customer preferences.

Activities related to the acquisition or lease of tangible assets
These operations involve acquiring buildings, machinery, and equipment, either through purchase, leasing, or in-house manufacturing, and these assets are kept on the balance sheets for more than a year. In national accounts, this falls under gross fixed capital formation. Payments for cloud services to use assets are also included.

Innovation management
Innovation management involves systematic planning, administration, and control of internal and external resources for innovation, including allocation of resources, organization of responsibilities and

decision-making, collaboration with external partners, integration of external inputs, monitoring of results, and learning from experience. It also includes defining policies, goals, objectives, procedures, structures, roles, and responsibilities for dealing with innovation and assessing and reviewing them. Information on innovation management is useful for evaluating the effectiveness of spending on innovation activities.

3.2. Changes that are not Innovations

This section describes changes that cannot be considered innovation, or can only be considered innovation if specific conditions are met. Innovation must be implemented and substantially different from the organization's previous products or processes.

• Routine modifications or upgrades, including software updates that only correct coding flaws, do not constitute product innovation.

• Replacing or extending existing capital with identical models, small extensions, or modifications to existing equipment or software is not an innovation. New equipment or expansions must be brand new to the company and represent a significant improvement in specifications.

• Modest aesthetic alterations, such as a colour change or slight shape change, do not meet the "substantial difference" standard and are not product innovations.

• One-of-a-kind, typically complex goods or services created by companies that specialize in bespoke manufacturing are not product innovations unless they have significant differences from previous products.

• A concept, prototype, or model of a product that does not yet exist is generally not considered product innovation because it does not meet the implementation criteria.

• The outputs of creative and professional service firms, such as client reports, novels, and films, are not always innovative for the companies that create them. For example, a consulting firm's report summarizing the findings of a design project completed for a customer without key novelty components is not a product innovation for the consulting business.

The Innovation Framework involves four steps: Acquisition, Implementation, Validation, and Improvement. Acquisition involves searching for innovation from various sources. Implementation involves defining testbeds, datasets, KPIs, and success criteria.

Validation requires a TRL8 readiness level. Improvement requires a TRL9 readiness level.

3.3. Acquisition

R&D is one way to generate innovations and acquire knowledge for innovation, but other methods include market research, process engineering, and analyzing user data. Information can also be gathered without a specific application in mind to help develop and evaluate options for future actions.

3.4. Implementation

For an idea to be considered an innovation, it must be implemented and made accessible to potential users. This distinguishes it from inventions or prototypes. Innovations must contain characteristics not previously available to users. The diffusion of information is important in explaining the rate at which new technology spreads and how quickly first responders adopt new technology.

3.5. Validation

Value is an implicit goal of innovation that provides different benefits to stakeholders, but its realization is uncertain and can only be fully assessed after implementation. Measures and analytical strategies are used to trace innovation outcomes after a suitable time. Outcome measures are important for understanding the impacts of innovation, especially for government policy initiatives promoting socially desirable outcomes. However, innovation outcomes are uncertain and heterogeneous, so value cannot be guaranteed.

3.6. Improvement

Activities that follow the implementation of an innovation can lead to minor or radical improvements, including fundamental redesigns or major improvements that may lead to new innovations. Post-implementation reviews can also result in the abandonment of innovations that are not successful or do not meet expectations. In some cases, these follow-on efforts may themselves result in new innovations.

4. Methodology

Our team is conducting interviews with police departments in EU member states with specialized law enforcement agencies (LEAs) for cybercrime. We will be gathering insights on the procedures, practices, and challenges of LEAs in combating cybercrime. We have received information on specialized LEAs from seven EU countries, including Belgium, Malta, France, Denmark, Latvia, Portugal, and Sweden, providing a diverse range of approaches to tackling cybercrime. Through these interviews, we hope to gain a comprehensive understanding of the strategies and tactics used by LEAs to fight cybercrime.

The interviews with these specialized LEAs will provide a wealth of information regarding their organization, budgeting, operations, and challenges in the area of cybercrime prevention and investigation. By analyzing this information, we aim to identify best practices and areas for improvement in the fight against cybercrime across the EU.

Overall, our initiative to conduct interviews with specialized LEAs for cybercrime across EU member states represents a significant effort to improve our understanding of this critical issue and identify strategies to address it effectively.

Cybercrime is a growing concern worldwide, and the EU has been actively working to combat it through various initiatives and policies. The EU has established a Cybercrime Programme Office (C3), which coordinates and supports the efforts of member states in fighting cybercrime. Many EU countries have also set up specialized LEAs for cybercrime to deal with the increasing number and complexity of cybercrimes.

Conducting interviews with the police departments of EU countries that have Cybercrime LEAs can provide valuable insights into the challenges faced by law enforcement in combatting cybercrime. The interviews can help to identify the best practices, strategies, and tools used by these departments, as well as the areas where they require additional support or resources. This information can be used to inform the development of policies, guidelines, and training programs aimed at improving the capacity of LEAs to respond to cybercrime.

In conclusion, securing interviews with the police departments of EU countries with Cybercrime LEAs is an important step in understanding the challenges and opportunities in combatting cybercrime in the EU. The information gathered through these interviews can inform the development of policies and training programs aimed at improving the capacity of LEAs to respond to cybercrime.

5. Interview questions

In order to define how innovation uptake can be more effective we have invited 57 representatives of different LEA departments that fight cybercrime in order to give us their own views in the following questions during a 1-to-1 online interview:

1. Do you have innovation management unit in your police force?

    1.1. What are the specific responsibilities of the members of the innovation management team?

    1.2. What is the composition of this team in terms of the number of members?

    1.3. What areas of expertise do the members possess?

    1.4. What additional topics should be explored based on the responses to the previous questions?

2. What is your budget for pilot testing and implementation of new tools/methodologies against cybercrimes?

    2.1 Protocols for securing funding?

    2.2 Budgetary constraints?

    2.3 Administrative or other impediments?

    2.4 Annual budget allocation?

    2.5 Procurement timelines post product selection?

    2.6 Additional areas of inquiry based on prior responses?

3. Which legal procedures do you follow for purchasing new innovative tools or services?

    For example, Pre-Commercial Procurement (PCP) or Public Procurement of Innovative Solutions (PPIs) or other?

6. RESULTS (anonymized)

6.1 Sweden

6.1.1 Interview results

According to the information provided, the Swedish police department has a specific budget allocated for pilot testing and implementing new tools and methodologies to combat cybercrimes. The procurement process for new tools can typically take between 2-12 months, depending on factors such as cost and whether licensing or a single payment is required. If funds are available, the process can be completed within 1-2 months, but bureaucracy may cause delays.

One challenge faced by the department is acquiring funding for digital forensics tools. This makes it difficult to plan for yearly licenses. Digital forensics may also be considered a small area of policy, making it challenging to secure funding when other areas may be prioritized. Therefore, exposure to the right channels within the force is crucial for obtaining funding and resources.

To ensure successful implementation of new tools, the department emphasizes the need for online education, a team with expertise in forensics and business development, and engineers with computer and network infrastructure expertise to facilitate the process. Forensics detectives will also be required to operate the tool effectively.

The department is confident that they will receive 100% of the tools required to carry out their work effectively. By investing in these new tools and methodologies, the Swedish police department is better equipped to protect citizens' digital lives and keep them safe from cyber threats. The department remains committed to its mission of providing a safe and secure environment for the people of Sweden, and these new tools are a significant step towards achieving that goal.

6.1.2 Summary

Answers related to the innovation management unit:

1.1. The specific responsibilities of the members of the innovation management team

1.2. The composition of this team in terms of the number of members

1.3. The areas of expertise possessed by the members

1.4. Additional topics that should be explored based on the responses to the previous questions

Answers related to budget for pilot testing and implementation of new tools/methodologies against cybercrimes:

2.1. Protocols for securing funding

2.2. Budgetary constraints

2.3. Administrative or other impediments

2.4. Annual budget allocation

2.5. Procurement timelines post product selection

2.6. Additional areas of inquiry based on prior responses

Legal procedures followed for purchasing new innovative tools or services are Pre-Commercial Procurement (PCP) or Public Procurement of Innovative Solutions (PPIs) or other.

6.2 Malta

6.2.1 Interview results

Law enforcement agencies use digital forensic tools such as Cellebrite and XRY to extract data from mobile devices. They receive recommendations on enhancing their capabilities from training programs such as OLAF, CEPOL, and Europol, and an online cybercrime unit with three departments has recently been founded. However, the agencies face a shortage of human resources in critical areas such as mobile or computer forensic, criminology, and IT. Networking and periodic meetings with other agencies play a vital role in enhancing their effectiveness. The procurement process of new tools and methodologies depends on funds' availability and can take 1-2 months, and transparency is essential to expedite the process. Law enforcement agencies follow established procurement procedures and guidelines, prioritizing technical specifications, price, and obtaining approval from relevant departments and authorities while using European funding and national funds with quotations and business case reports.

An ideal approach would be to collaborate with law enforcement agencies (LEAs) from other countries and undergo annual online training via recorded sessions. There is a significant need for AI software that can analyze photos related to crimes against child exploitation.

6.2.2 Summary

1. Do you have innovation management unit in your police force?
   - There is no information provided regarding the presence or absence of an innovation management unit in the police force.

   1.1. What are the specific responsibilities of the members of the innovation management team?
   - There is no information provided regarding the specific responsibilities of the members of an innovation management team.

   1.2. What is the composition of this team in terms of the number of members?
   - There is no information provided regarding the composition of an innovation management team in terms of the number of members.

   1.3. What areas of expertise do the members possess?
   - There is no information provided regarding the areas of expertise possessed by the members of an innovation management team.

   1.4. What additional topics should be explored based on the responses to the previous questions?
   - As there is no information provided regarding the existence or composition of an innovation management team, no additional topics can be explored.

2. What is your budget for pilot testing and implementation of new tools/methodologies against cybercrimes?
   - There is no information provided regarding the budget for pilot testing and implementation of new tools/methodologies against cybercrimes.

   2.1 Protocols for securing funding.
   - The procurement process for new tools and services involves following established procurement procedures and guidelines and obtaining approval from relevant departments and authorities.

   2.2 Budgetary constraints.
   - There is no information provided regarding budgetary constraints.

   2.3 Administrative or other impediments.
   - There is no information provided regarding administrative or other impediments.

   2.4 Annual budget allocation.
   - There is no information provided regarding annual budget allocation for new tools and services.

   2.5 Procurement timelines post product selection.
   - The timeline for acquiring new tools/methodologies for combating cybercrimes depends on the availability of funds. If funds are available, the procurement process can be completed within 1-2 months. However, if funds are not available, the timeline depends on factors such as the cost and uniqueness of the tool and whether it requires licensing or a single payment. In such cases, the procurement process could take longer.

   2.6 Additional areas of inquiry based on prior responses.
   - Possible additional areas of inquiry could include further details on the procurement process, funding sources and mechanisms, and the specific factors that affect the timeline for acquiring new tools and methodologies.
   - Which legal procedures do you follow for purchasing new innovative tools or services e.g., Pre-Commercial Procurement (PCP) or Public Procurement of Innovative Solutions (PPIs) or other?
   - There is no information provided regarding the specific legal procedures followed for purchasing new innovative tools or services. The procurement process involves following established procurement procedures and guidelines, prioritizing technical specifications, price, and obtaining approval from relevant departments and authorities.

6.3 Latvia

6.3.1 Interview results

There is an innovation management unit in the police force consisting of experts in various fields such as Forensics or IT. The unit conducts market research to identify new tools or methodologies against Cybercrime and shares their findings with other LEAs.

The team consists of 25 analysts consisting of software engineers and data analysts who possess expertise in various areas, including mobile phones, evidence analysis of all kinds of crimes, cryptocurrency, and malware analysis. The team has specific budget allocated for pilot testing and implementing new tools/methodologies against cybercrimes.

The legal procedures for purchasing new innovative tools or services involve an open procurement process that includes defining the technical specifications required, announcing tenders on their website, and interested parties can apply by sending their credentials and offers. Several reports have been sent to the Internal Affairs Ministry, and the agency is awaiting approval to move forward. Additional areas of inquiry could include further details on the budget allocation and procurement process, sources of funding, and the specific factors that affect the timeline for acquiring new tools and methodologies.

6.3.2 Summary

1. Do you have innovation management unit in your police force?

    - Yes, there is an innovation management unit in the police force consisting of experts in various fields such as Forensics or IT. The unit conducts market research to identify new tools or methodologies against Cybercrime and shares their findings with other LEAs. 1.1. What are the specific responsibilities of the members of the innovation management team?

    - The specific responsibilities of the members of the innovation management team include conducting market research to identify new tools or methodologies against Cybercrime, sharing their findings with other LEAs, and exploring and assessing the possibilities of new tools. 1.2. What is the composition of this team in terms of the number of members?

    - The team consists of 25 analysts consisting of software engineers and data analysts. 1.3. What areas of expertise do the members possess?

    - The members possess expertise in various areas, including mobile phones, evidence analysis of all kinds of crimes (e.g., burglary), cryptocurrency, and malware analysis. 1.4. What additional topics should be explored based on the responses to the previous questions?

    - Possible additional topics of inquiry could include further details on the roles and responsibilities of the innovation management unit, the process of sharing findings with other LEAs, and the development of in-house big data analytics.

2. What is your budget for pilot testing and implementation of new tools/methodologies against cybercrimes?
    - The budget allocated for pilot testing and implementing new tools/methodologies against cybercrimes is not exceeding 0.5 million.
    - There is no information provided regarding protocols for securing funding. 2.2 Budgetary constraints.
    - Several reports have been sent to the Internal Affairs Ministry, and the agency is awaiting approval to move forward. The authorities expect to acquire the necessary tools for the project as there is a 100% commitment to obtaining them. 2.4 Annual budget allocation.
    - There is no information provided regarding annual budget allocation for new tools and services. 2.5 Procurement timelines post product selection.
    - The timeline from the tender to the product being acquired is typically about two months. 2.6 Additional areas of inquiry based on prior responses.
    - Possible additional areas of inquiry could include further details on the budget allocation and procurement process, sources of funding, and the specific factors that affect the timeline for acquiring new tools and methodologies.

3. Which legal procedures do you follow for purchasing new innovative tools or services e.g., Pre-Commercial Procurement (PCP) or Public Procurement of Innovative Solutions (PPIs) or other?

    - The legal procedures for purchasing new innovative tools or services involve an open procurement process that includes defining the technical specifications required. The authorities announce tenders on their website, and interested parties can apply by sending their credentials, such as tax department details, and offers. The timeline from the tender to the product being acquired is typically about two months.

6.4 Portugal

6.4.1 Interview results

The process of identifying and acquiring new tools and methodologies against cybercrime in law enforcement agencies involves identifying the need, following a chain of command and acquiring the necessary funding.

The innovation management unit in the police force is responsible for conducting market research to identify new tools and sharing their findings with other agencies. However, they face challenges such as a shortage of personnel, the need for expensive training, and difficulties in securing funding. The authorities use both European and local funding to acquire new tools, but only part of requests for funding are successful.

The legal procedures for purchasing new innovative tools or services involve the Ministry of Internal Affairs opening procurements and following established procurement procedures and guidelines.

Overall, these findings highlight the need to prioritize funding and personnel and streamline the procurement process to combat cybercrime effectively.

6.4.2 Summary

1. Innovation Management Unit:
    - Yes, there is an innovation management unit in the police force.
    - The specific responsibilities of the members include identifying the need for new tools and methodologies against Cybercrime, identifying the tool, and following a chain of command that ends with the Ministry of Internal Affairs.
    - The composition of the team consists of an unknown number of members with varying areas of expertise.
    - Additional topics that could be explored include the team's decision-making process, the types of tools/methodologies used, and how the team collaborates with other units in the police force.
2. Budget for Pilot Testing and Implementation of New Tools/Methodologies against Cybercrimes:
    - The funding for these activities comes from European and local sources.
    - The authorities faced some difficulties in acquiring funds due to a limited time frame, and requests for funding were successful only four times out of seven attempts.
    - Yearly licenses for the tools are difficult to explain to the government, and the renovations start at the beginning of the year and take off the year in November.
    - Challenging to ask for funding as they prioritize some areas and may leave out others.
    - The timeline for acquiring the product is typically about two months.
3. Legal Procedures for Purchasing New Innovative Tools or Services:
    - The legal procedures for purchasing new innovative tools or services involve the Ministry of Internal Affairs opening procurements.
    - The process begins with defining the technical specifications required for the tool or service, followed by announcing tenders on their website.
    - Interested parties can then apply by sending their credentials and offers.
    - Although there was no specific mention of Pre-Commercial Procurement (PCP) or Public Procurement of Innovative Solutions (PPIs), the authorities follow established procurement procedures and guidelines to purchase new tools and services.

6.5 Belgium

6.5.1 Interview results

From the information provided, it can be concluded that the police force has an innovation management unit responsible for identifying the need for new tools and methodologies against cybercrime, collaborating with other countries and LEAs, reviewing digital forensics publications, and conducting R&D for developing new technologies. Protection readiness is also crucial when using any new database. However, the budget for pilot testing and implementation of new tools is subject to bureaucratic delays. To secure funding, the prosecutor offers the budget, and investigators with expertise in cybercrime and computer science provide the technical specifications. The budgetary constraints are challenging, and funding comes from European and national sources, but there are difficulties in acquiring funds due to a limited time frame. Despite this, the authorities follow established procurement procedures and guidelines to purchase new tools and services.

The legal procedures involve preparing technical specifications and sending them to the innovation officers, and the Ministry of Internal Affairs opens procurement, announcing tenders on their website. Although there is a need to further explore the decision-making process and how the innovation management unit collaborates with other units, the police force is committed to acquiring new tools and methodologies for effectively combating cybercrime.

6.5.2 Summary

1. Innovation Management Unit:
    - Yes, there is an innovation management unit in the police force.
    - The specific responsibilities of the members include identifying the need for new tools and methodologies against cybercrime, collaborating with other countries and LEAs to find out what they are using, reviewing digital forensics publications and following well-known companies and mailing groups, and doing R&D for developing new technologies, including developing software within a police officer.
    - The composition of the team is unknown in terms of the number of members and areas of expertise.
    - Additional topics that could be explored include the team's decision-making process, the types of tools/methodologies used, and how the team collaborates with other units in the police force.
2. Budget for Pilot Testing and Implementation of New Tools/Methodologies against Cybercrimes:
    - The budget for pilot testing and implementation of new tools is not clear and subject to bureaucratic delays.
    - The prosecutor requests a new tool and offers the budget, and investigators with expertise in cybercrime and computer science provide the technical specifications.
    - The budgetary constraints are challenging, and funding comes from European and national sources, but the authorities face difficulties in acquiring funds due to a limited time frame.
    - Additionally, yearly licenses for the tools are difficult to explain to the government, and renovations start at the beginning of the year and take off the year in November.
    - The protocols for securing funding, administrative or other impediments, annual budget allocation, and procurement timelines post-product selection are areas of inquiry based on the prior responses.
3. Legal Procedures for Purchasing New Innovative Tools or Services:
    - The legal procedures for purchasing new innovative tools or services involve the project officer preparing the technical specifications required for the tool or service and sending it to the innovation officers.
    - The Ministry of Internal Affairs then opens procurement, announcing tenders on their website, and interested parties can apply by sending their credentials and offers.
    - Although there was no specific mention of Pre-Commercial Procurement (PCP) or Public Procurement of Innovative Solutions (PPIs), the authorities follow established procurement procedures and guidelines to purchase new tools and services.

6.6 France

6.6.1 Interview results

From the information provided, it can be concluded that the police force has an innovation management unit responsible for developing and testing new technologies to combat cybercrime. The new technologies are tested before being adopted by the whole police force. The testing procedure involves first being tested in forensics before being sent to cybercrime units and then other departments. However, the innovation management unit does not engage too much in international collaborations due to being too busy with investigations. The police force has enough resources to obtain new tools if needed, but there is no clear answer to what the budget for pilot testing and implementation of new tools is.

The police force follows French laws for direct allocation of a Tender when purchasing new innovative tools or services and only purchases the tool when it is already on the market. There are no legal problems for using a new tool, and the police force talks to prosecutors to inform them and follow any necessary procedures.

6.6.2 Summary

1. There is an innovation management unit in the police force.
    - The team is responsible for developing and testing new technologies to combat cybercrime.
    - The members possess expertise in forensics and cybercrime.
    - Additional topics to explore may include the training process for the team members and any plans for expanding the team or its scope of work.
2. There is no clear answer regarding the budget for pilot testing and implementation of new tools. However, the police force seems to have enough resources to obtain necessary tools.
    - 2.1. The police force follows French laws for direct allocation of a Tender when purchasing new tools or services.
    - 2.2. Budgetary constraints are not mentioned explicitly.
    - 2.3. Administrative impediments are not mentioned explicitly.
    - 2.4. Annual budget allocation is not provided.
    - 2.5. The police force only purchases tools when they are already on the market.
    - 2.6. Additional areas of inquiry may include the effectiveness of the implemented tools and how the budget allocation process can be improved.
3. The police force follows French laws for direct allocation of a Tender when purchasing new innovative tools or services.
    - No specific mention of Pre-Commercial Procurement (PCP) or Public Procurement of Innovative Solutions (PPIs) was provided in the answers.

6.7 Denmark

6.7.1 Interview results

The Innovation management leader identifies the need for new tools and presents their technical specifications and potential usage to Law Enforcement Agencies in all districts in Denmark through monthly meetings, facilitating the decision-making process.

The budget for pilot testing and implementation depends on the complexity and scale of the tool, and acquiring new tools can take 6-12 months. Bureaucracy can delay the budget. The Danish police department can obtain the necessary tools within a reasonable time frame. If funds are available, the procurement process can be completed within 6 months, but if not, the timeline depends on factors such as cost, uniqueness, and licensing/payment requirements.

6.7.2 Summary

1. Do you have an innovation management unit in your police force?
    - Yes, there is an Innovation management leader who identifies the need for new tools and presents them to Law Enforcement Agencies (LEAs) in all districts in Denmark through monthly meetings.
2. What are the specific responsibilities of the members of the innovation management team?
    - Identifying and researching new tools, technologies, and methodologies
    - Presenting technical specifications and potential usage to LEAs
    - Facilitating decision-making processes for acquiring new tools
3. What is the composition of this team in terms of the number of members?
    - Not specified
4. What areas of expertise do the members possess?
    - Not specified
5. What additional topics should be explored based on the responses to the previous questions?
    - Team members' backgrounds and expertise
    - Collaboration with external stakeholders and experts
    - Evaluation criteria for new tools and technologies
6. What is your budget for pilot testing and implementation of new tools/methodologies against cybercrimes?
    - Limited budget (not specified)
7. Protocols for securing funding.
    - Not specified
8. Budgetary constraints
    - Bureaucracy delays the budget
9. Administrative or other impediments
    - Not specified
10. Annual budget allocation
    - Not specified
11. Procurement timelines post product selection
    - If funds are available, the procurement process can be completed within 6 months. If funds are not available, the timeline depends on factors such as cost, uniqueness, and licensing/payment requirements.

12. Additional areas of inquiry based on prior responses
    - Specific funding sources and grant opportunities
    - Internal processes for budget approval
    - Prioritization of tools and methodologies
13. Which legal procedures do you follow for purchasing new innovative tools or services, e.g., Pre-Commercial Procurement (PCP) or Public Procurement of Innovative Solutions (PPIs) or other?
    - Not specified

7. Summary of conclusions

Common conclusions between the countries:

1. Budget constraints: All countries mentioned face budget constraints and challenges in acquiring funding for digital forensics tools. Funding comes from both European and local sources, and the budget for pilot testing and implementing new tools is often small.
2. Bureaucracy and procurement process: The procurement process for acquiring new tools can be lengthy and bureaucratic, taking anywhere from 1 to 12 months depending on factors such as cost, licensing, and payment requirements. Transparency and proper adherence to established procurement procedures and guidelines are crucial to expedite the process.
3. Innovation management units: Most countries have dedicated innovation management units or teams responsible for identifying the need for new tools, conducting market research, and sharing their findings with other law enforcement agencies. These units face challenges such as a shortage of personnel and the need for expensive training.
4. Collaboration and networking: Networking and periodic meetings with other agencies play a vital role in enhancing the effectiveness of law enforcement agencies. Collaborating with law enforcement agencies from other countries and undergoing annual online training can help in sharing best practices and improving capabilities.
5. Human resources: Several countries face a shortage of human resources in critical areas such as mobile or computer forensic, criminology, and IT. Investing in personnel training and development is essential for the successful implementation of new tools and methodologies.
6. Legal procedures: Countries follow their respective legal procedures for purchasing new innovative tools or services, which generally involve defining technical specifications, announcing tenders, and obtaining approval from relevant departments and authorities.

Overall, the common conclusions suggest that law enforcement agencies in these countries face similar challenges in terms of budget constraints, bureaucracy, procurement processes, human resources, and legal procedures. Addressing these challenges requires prioritizing funding and personnel, streamlining the procurement process, and fostering collaboration between agencies to effectively combat cybercrime.

8. Statistics for countries involved in this survey.

Statistics on the specialized law enforcement agencies (LEAs) for cybercrime in European Union (EU) countries indicate that many member states have established such agencies to address the growing threat of cybercrime. The establishment of specialized cybercrime units within police departments is becoming increasingly common as the complexity and frequency of cybercrimes continue to rise.

1. Belgium established its Cybercrime Unit in 1999, which is responsible for investigating and preventing cybercrime in the country. The unit is composed of specialists in digital forensics, network security, and cybercrime investigations.

2. In Malta, the Cybercrime Unit was established in 2014, which is responsible for investigating and prosecuting cybercrimes[4].

3. France has one of the most advanced Cybercrime LEAs in the EU, known as the Central Office for Combating Cybercrime (OCLCTIC). It is responsible for investigating cybercrimes and coordinating the efforts of other French law enforcement agencies in this area.

4. Denmark's National Cyber Crime Center (NC3) was established in 2012 and is responsible for coordinating and supporting the efforts of the Danish police in investigating cybercrimes[5].

5. Latvia established its Cybercrime Unit in 2012, which is responsible for preventing and investigating cybercrimes, including hacking, fraud, and identity theft.

6. In Portugal, the Judiciary Police (PJ) has a Cybercrime Unit that was established in 2008 and is responsible for investigating cybercrimes and supporting other law enforcement agencies in this area[6].
7. Sweden has a specialized cybercrime unit within its National Bureau of Investigation (NBI), which was established in 2014. The unit is responsible for investigating cybercrimes and coordinating the efforts of other Swedish law enforcement agencies in this area[7].

[4] Federal Police of Belgium. (2021). Cyber Crime Unit. Retrieved from https://www.politie.be/en/about_us/organisation/directorate_general_of_the_police/commissariat_general_criminal_investigation_department/specialised_units/cyber_crime_unit

Europol. (2019). National Cybercrime Units in the EU. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/National%20Cybercrime%20Units%20in%20the%20EU.pdf

[5] Central Office for Combating Cybercrime (OCLCTIC). (n.d.). Presentation. Retrieved from https://www.interieur.gouv.fr/content/download/73716/527270/file/1%20-%20Presentation%20OCLCTIC.pdf

Europol. (2019). National Cybercrime Units in the EU. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/National%20Cybercrime%20Units%20in%20the%20EU.pdf

[6] State Police of Latvia. (n.d.). Cybercrime Unit. Retrieved from https://www.vp.gov.lv/en/about-us/structure/investigation-department/cybercrime-unit

Europol. (2019). National Cybercrime Units in the EU. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/National%20Cybercrime%20Units%20in

[7] Swedish Police Authority. (n.d.). National Cybercrime Center. Retrieved from https://www.polisen.se/en/om-polisen/polismyndigheten/polismyndigheten-i-stockholms-lan/avdelningar/nationellt-cyberbrottscentrum/

Europol. (2019). National Cybercrime Units in the EU. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/National%20Cybercrime%20Units%20in%20the%2

8. In Portugal, the Judiciary Police (PJ) has a Cybercrime Unit that was established in 2008 and is responsible for investigating cybercrimes and supporting other law enforcement agencies in this area. The PJ's Cybercrime Unit collaborates with other Portuguese law enforcement agencies and international partners to investigate cybercrime and bring cybercriminals to justice[8].

[8] Judiciary Police. (n.d.). Cyber Crime Investigation Unit. Retrieved from https://www.policiajudiciaria.pt/paginas/ct-ciber

Europol. (2019). National Cybercrime Units in the EU. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/National%20Cybercrime%20Units%20in%20the%20EU.pdf

9. Conclusions of 2nd Annual Innovation Uptake

In conclusion, specialized law enforcement agencies (LEAs) for cybercrime have been established across European Union (EU) countries to address the growing threat of cybercrime. The establishment of these specialized cybercrime units within police departments is increasingly common due to the rising complexity and frequency of cybercrimes. Countries including Belgium, Malta, France, Denmark, Latvia, Sweden, and Portugal have set up cybercrime units responsible for investigating and preventing cybercrimes.

These specialized cybercrime units, with their dedicated teams of experts in digital forensics, network security, and cybercrime investigations, play a crucial role in investigating and preventing cybercrimes. They collaborate with other national law enforcement agencies and international partners to share best practices, resources, and expertise, making them valuable assets in the fight against cybercrime.

However, countries face common challenges in terms of budget constraints, bureaucracy, procurement processes, human resources, and legal procedures when acquiring and implementing new tools and methodologies to combat cybercrime. To address these challenges, LEAs need to prioritize funding and personnel, streamline the procurement process, and foster collaboration between agencies.