

Policy Paper

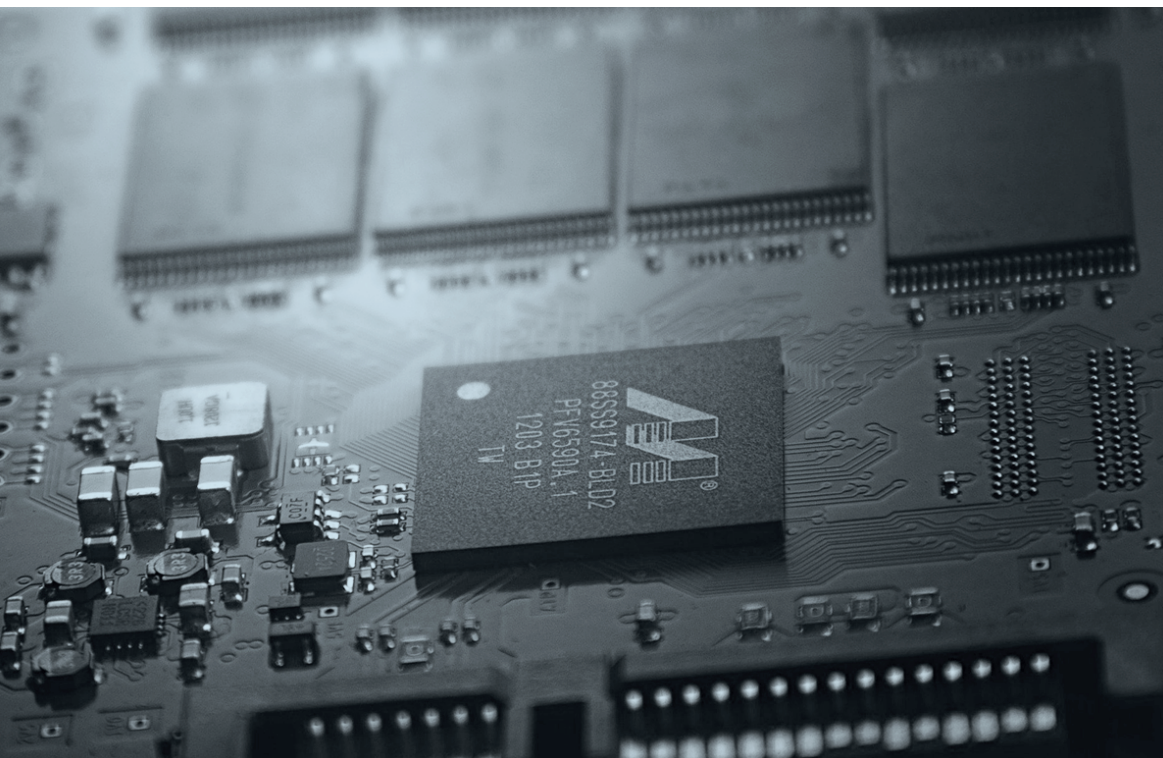
Big Data, 5G and AI

How Europol could help von der Leyen achieve her goals

19 February 2020

Franca König, Guest Author

#vdLCommission
#Europol
#AEuropeFitForThe
DigitalAge
#Digitalisation



Commission President Ursula von der Leyen has pledged to make Europe ‘fit for the digital age’, including in the areas of big data, 5G and artificial intelligence. On March 9, her first 100 days in office will be over and measured against her agenda for the legislative period 2019–2024. While the course has been set for an innovative and competitive EU as regards digitalisation and cyber, the Commission’s approach has so far lacked a security perspective. This Policy Paper explains why the inclusion of a security dimension is crucial and how Europol, the EU’s agency for police cooperation, could help von der Leyen to this end.

Executive summary

The new European Commission has set an ambitious agenda for itself, especially in the areas of digitalisation and cyber. With Commission President von der Leyen's 100th day in office fast approaching, various measures and processes are currently being rolled out to ensure she reaches her goals within the next four years. Three key targets are the improvement of information exchange, the establishment of joint 5G standards and the development of a European ethical approach to artificial intelligence (AI).

In view of the increasing importance of digitalisation and cyber in virtually all areas of life, von der Leyen's agenda comes at the right time. Making the EU 'fit for the digital age' whilst safeguarding ethical boundaries will empower European businesses and citizens alike to fully reap the benefits of new technologies such as 5G and AI. At the same time, the Commission's focus should not lie exclusively on socioeconomic interests and innovation. The challenges posed by big data and digital technologies will also continue to grow over the coming years, and these include an increased attack surface and potential for manipulation or criminal and terrorist abuse. Addressing the security dimension of digitalisation and cyber in the European debate and approach to new technologies will thus be of paramount importance in making sure innovation does not come at the expense of security.

Europol, the EU's Agency for Law Enforcement Cooperation, could help mitigate this risk and contribute to the achievement of von der Leyen's goals from a law enforcement perspective. While other actors and agencies might of course offer a more specialised point of view – such as on the operational management of the EU's large-scale IT systems or its cybersecurity – Europol has the advantage of a cross-sectional overview, owing to its very extensive involvement in most areas of internal security. As the EU's criminal intelligence hub, it can offer two decades of experience in information exchange and data analysis assisting Member States and their police authorities. Apart from best practices and a law enforcement voice, Europol brings practical tools and threat assessment capabilities to the table. Its Cybercrime Centre and Internet Referral Unit (amongst others) have been focussing on the security aspects of digitalisation and cyber, and how to resolve concrete problems and risks, for example related to big data management or the use of encryption and anonymity online for illicit activities.

About the author:
Franca König is an expert on EU security with a focus on police cooperation.

To ensure that the EU is not only fit for the digital age, but also that it is capable of protecting its citizens, the European Commission would be well advised to consider the security aspects of new technologies and their application in the EU. Whether and to what extent Europol will support it in this regard – and concretely help von der Leyen achieve her goals related to big data, 5G and AI – ultimately depends on three key factors:

1. the **inclusion** of the agency in the relevant discussions **at EU level**;
2. the **formal strengthening** of Europol's role as the EU criminal intelligence hub in the context of new legislation;
3. the **guarantee of sufficient resources** (the availability of money, data, posts) for the agency to fulfil its tasks.

Table of Contents

1	Why the digitalisation debate needs a security dimension.....	1
2	‘Digitalisation and cyber’ – how to deal with data, 5G and AI?	2
2.1	Target 1: Handling data – From ‘need to know’ to ‘need to share’	2
2.2	Target 2: ‘Joint standards for our 5G networks’	4
2.3	Target 3: ‘A coordinated European approach on the human and ethical implications of AI’	6
3	Von der Leyen’s first 100 days and beyond: where Europol should be headed.....	7
	On the same topic	9

1 Why the digitalisation debate needs a security dimension

2020 marks a breaking point for the EU with multiple challenges and opportunities ahead. Some of them will undoubtedly lie in the realms of cyber and digitalisation. In the past few years alone, we have produced more data than in all of human history combined.¹ The use of new and digital technologies is spreading at an ever-accelerating pace: the Internet of Things (IoT), Artificial Intelligence (AI) and 5G are rapidly conquering all areas of life. They hold the potential to help solve numerous problems, such as managing public services and resources, tailoring treatments in the health sector, and achieving climate neutrality.

The new European Commission has come to that same conclusion. Its organisational set-up demonstrates how important it considers this topic, with Digital Commissioner Margrethe Vestager having been appointed Executive Vice-President. Commission President Ursula von der Leyen has made digitalisation and cyber political priorities for the legislative period 2019–2024. Her *Agenda for Europe* not only features digital technologies throughout, it dedicates an entire section (‘A Europe fit for the digital age’) to the issue while setting ambitious targets for the EU.²

Notwithstanding the potential benefits of a digitalised Europe, there is a flip side to this development that has perhaps been somewhat neglected, if not partially omitted from on-going discussions: a more digitalised society in turn means a deeper interconnectedness among all areas of life and thereby a widening of the potential attack surface first and foremost, and secondly, an intensification of the potential damage from criminal and terrorist attacks in such an environment. The more we rely on digital technologies, the more crucial it becomes to thoroughly assess their impact and mitigate risks or harm where necessary. Many of the Commission’s political targets will likewise affect the area of Justice and Home Affairs (JHA) and the security of the Union and its citizens. Including a security dimension in the digitalisation debate thus seems especially vital. Here, the Commission would be well advised to draw and build on existing capabilities and expertise, rather than starting from scratch or duplicating initiatives in an already crowded policy field.

This holds especially true because von der Leyen’s agenda comes at a time when European police cooperation is stronger than ever. Europol, the EU’s official agency for police cooperation, just celebrated its 20-year anniversary last year.³ Since it took up operations in 1999, it has grown from an intergovernmental organisation with a workforce of barely 300, to a well-established EU agency with around 1,300 people currently working at its headquarters in The Hague.⁴ Today, Europol supports Member States in virtually all areas of internal security and home affairs. As the EU’s central criminal intelligence hub, digital and cyber elements

“The more we rely on digital technologies, the more crucial it becomes to thoroughly assess their impact and mitigate risks or harm.”

¹ Marr, Bernard. “How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read.” *Forbes*, May 21, 2018. Accessed February 10, 2020.

² Von der Leyen, Ursula. “A Union that strives for more: My agenda for Europe. Political guidelines for the next European Commission (2019–2024).” July 16, 2019. Accessed November 8, 2019.

³ Europol. “Europol 20 years.” Accessed November 8, 2019.

⁴ Europol. “Statistics & Data – Europol Staff Numbers.” Accessed November 8, 2019.

have played a key role in most of its activities and mandated areas since the beginning. Its long track record in this field, including a dedicated cybercrime centre and internet unit, should make it well equipped to help von der Leyen achieve her goals. This policy brief explains why including a security dimension in the areas of digitalisation and cyber is essential, and how Europol could support the new Commission President.

2 ‘Digitalisation and cyber’ – how to deal with data, 5G and AI?

Under the heading “A Europe fit for the digital age,” von der Leyen addresses the importance of digitalisation and cyber. In contrast to ‘digitisation’ (the process of transforming analogue data to the digital), ‘digitalisation’ refers to its impact on social interactions and structures.⁵ ‘Cyber’ describes the virtual space created by computers. In relation to these concepts, von der Leyen mentions three concrete targets that also matter for European police cooperation and which Europol could contribute to accomplishing: improving information exchange, introducing joint standards for 5G networks, and a coordinated approach to AI.

2.1 Target 1: Handling data – From ‘need to know’ to ‘need to share’

Regarding the improvement of intra-EU information sharing, von der Leyen calls for a shift from a ‘need to know’ to a ‘need to share’ basis. This means moving from a system where data exchange only takes place when authorities require it (and the problem of identifying who actually needs to know what) to a system where everybody needs to share (at least the type of) information they possess so it can be accessed by authorised users if necessary.

Von der Leyen suggests achieving this through a ‘joint Cyber Unit.’ The relevance of Europol in this context – as the EU agency for police cooperation – is obvious. Among its key tasks are the facilitation of information exchange and coordination among competent authorities.⁶ As such, it can help to crucially enhance the sharing and availability of relevant data among EU Member States. Europol already possesses significant capabilities to this effect. For example, it administers several databases that can be searched and accessed by authorised law enforcement representatives and that contain a wide array of criminal information and intelligence on organised crime and terrorism. Since its inception, the number of Europol databases on the one hand, and the amount of information stored or processed by the agency on the other, have grown continuously.

Next to supporting the establishment of a principle of availability in EU information exchange, Europol could help improve the efficiency of data sharing. A sort of ‘joint Cyber Unit’ already exists at the agency, namely its European Cybercrime Centre (EC3). The EC3 brings together a variety of public and private stakeholders,

⁵ Brennen, Scott, and Kreiss, Daniel. “Digitalization and Digitization.” Culture Digitally, September 8, 2014. Accessed February 10, 2020.

⁶ European Commission. “Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.” May 11, 2016, pp. 64–65.

and assists law enforcement authorities through strategic analysis, capacity building and operational support. It was launched to address the need at EU level for a central point of contact and coordination in the fight against cybercrime. Europol thus possesses substantial experience in coordinating information exchange as well as organising and processing data based on the purpose for which it is intended (rather than its source). Its expertise on how to make information sharing not only easier and faster, but also safer in line with EU data protection rules, could help von der Leyen achieve secure and integrated data management at EU level and move information exchange towards the principle of availability rather than a ‘need to know’ basis.

Nevertheless, Europol remains focused on law enforcement and therefore limited. Most of the EU’s information systems are administered by eu-LISA, the EU Agency for the Operational Management of Large-Scale IT Systems. As these systems are also being partially automated and will continue to integrate new digital technologies, Europol alone cannot assist von der Leyen in the improvement of EU information exchange and the handling of big data. However, it could make best practices and lessons learned from the field of EU police cooperation available, for example from its experience in the management and analysis of big data related to illegal migration or radicalisation online.

To fully harness its expertise, von der Leyen should ensure that the agency gets a seat at the table when the interoperability of EU information systems is developed further. Making sure that information is not recorded multiple times or wrongly across different databases will be key, not only in the management of big data and the protection of European internal security, but also in the safeguarding of citizens’ personal data and privacy rights. To this end, Europol officials could undoubtedly offer a good share of expertise on “moving from data collection to data connection.”⁷ The agency has long advocated for (and has started an internal process) the restructuring of information storage and exchange around the principle of availability, i.e. shifting away from isolated data ‘silos’ towards a system of integrated data management.

For Europol to be able to support von der Leyen in establishing the principles of availability, efficiency and privacy within EU information exchange, Europol’s position as a central hub for the exchange of criminal information and intelligence should be further strengthened legally, and upgraded in terms of resources (i.e. money and posts). If all of the relevant available information is to be shared or coordinated via Europol, this can only succeed if the agency and its systems are sufficiently equipped to process the information they receive. This same logic applies to a possible ‘joint Cyber Unit’ and von der Leyen’s envisaged full digitalisation of the Commission.

Finally, the success or failure of any EU attempt at improving data sharing among Member States and different databases hinges on the willingness of domestic governments and security authorities to provide the relevant data, oversee its processing and protection at a central level, and adjust rules and regulations accordingly if necessary. However, while information exchange has come a long way, data collection and analysis still lag behind. Improving the exchange of information within the EU involves dealing with mass data and encryption, managing trust

“Europol officials could undoubtedly offer a good share of expertise on ‘moving from data collection to data connection.’”

⁷ European Council. “The future of EU Law Enforcement – Policy debate” (Council doc. 9393/19). May 17, 2019.

issues among the various agencies, and ensuring the adequate design of privacy rules. Europol or the Commission could not rise to such a challenge alone.

2.2 Target 2: 'Joint standards for our 5G networks'

"The fifth generation of telecommunication systems, or 5G, is considered to be one of the most critical building blocks of our digital economy and society over the next decades", Europol observed in the summer of 2019.⁸ The technology – expected to boost mobile internet speed by up to 100-fold and to be more reliable and efficient than 4G – promises a broad range of opportunities on the path towards an increasingly digital Europe, with expanding smart and interconnected electronic infrastructures, including the IoT.⁹

In 2016, the European Commission saw a "strategic opportunity" in this area and adopted a *5G for Europe* action plan that targeted the "launch of fully commercial 5G services in Europe by the end of 2020."¹⁰ Whereas various public and private partners had already been involved in talks by the Commission as far back as 2013, European law enforcement agencies were brought in "too late" according to Europol's Executive Director Catherine De Bolle: "[W]e need to be at the table where they discuss about the technological development, where they discuss standardisation."¹¹ If von der Leyen truly wants to *jointly* define standards for these new technologies that may act as a role model for global norms, she would be well advised to not only focus on citizens and businesses, but to bring law enforcement representatives into the loop and address security aspects.

This seems ever more crucial in view of the many challenges that 5G poses. In mid-2019, Europol published a report on the impact of potentially 'disruptive technologies' – such as AI, 5G and quantum computing – on the future of European internal security and policing. While 5G can undoubtedly contribute to better protection of users and their data, for example through direct communication between devices and end-to-end encryption, the same qualities may benefit malicious actors and cause adverse effects for law enforcement. To name but two problems: firstly, 5G complicates legally permissible investigation and surveillance by technical means. Police officers may be unable to identify and locate users, i.e. potential suspects and criminals. Secondly, 5G technology complicates lawful interception. The same qualities that make it faster and more flexible, such as network slicing or Multi-Access Edge Computing (where data is no longer processed in a centralised cloud but close to the user), equally restrict the information available and accessible to authorised police officers.

To reap the benefits of 5G, and protect citizens as well as businesses from its disruptive potential, any joint standards must go beyond commercial interest and

⁸ Europol. "Do criminals dream of electric sheep? How technology shapes the future of crime and law enforcement." 2019, p. 12. Accessed January 20, 2020.

⁹ Council of the European Union. "Position paper on 5G by Europol" (Council doc. 8268/19). Brussels, April 11, 2019.

¹⁰ European Commission. "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – 5G for Europe: An Action Plan" (COM(2016) 588 final). September 14, 2016, pp. 2 and 4.

¹¹ Deutsch, Anthony. "Police need intercept tools as mobile networks develop: Europol." Reuters, July 18, 2019. Accessed January 5, 2020.

innovation in the development of related technologies and networks. Europol could help develop both from a security perspective as well, not only through its inclusion in the respective discussions and working groups, but through practical input and tools for practitioners.

As problems of encryption are virtually omnipresent throughout all police work and in most investigations, von der Leyen should take a closer look at the agency's decryption platform and innovation lab for a more holistic view of 5G and the balance between freedom and security. Since 2018, Europol has hosted a decryption platform within its EC3 that deals with the role of encryption in criminal investigations. Next to assessing legal aspects, the unit provides operational support and develops free-of-charge decryption tools.¹² It could add important practical value to the debate on joint standards for 5G networks in the EU by raising the issue of law enforcement access to relevant data and highlighting concrete operational or technical obstacles and challenges.

Additionally, Europol is in the process of creating an innovation laboratory, which, JHA Ministers agreed in October, shall “act as an observatory of new technological developments and drive innovation” in the field of European internal security.¹³ The lab was envisaged in 2018, if not earlier, when Europol's Management Board made being “at the forefront of law enforcement innovation and research” a strategic priority.¹⁴ It has yet to be launched; a mere three posts are foreseen to begin with, according to Europol officials, and its further development will essentially depend on funding for Europol under the next multiannual financial framework. Nonetheless, such an innovation lab could represent a substantial asset in the further development of 5G, including methods of lawful interception, a topic on which Europol has already been gathering experts.¹⁵

Europol can help von der Leyen develop joint standards that not only make Europe fit for the digital age, but also protect its internal security and allow police officers to do their job. Nonetheless, there are limits, as its perspective will always remain primarily focused on the fight against crime and terrorism. At EU level, other players from the field of JHA should therefore be involved as well, including Eurojust, the EU Agency for Criminal Justice Cooperation, and the European Data Protection Supervisor (EDPS), to ensure adequate judicial and data protection frameworks. Ultimately, it will be up to the private sector to implement these standards as well as cooperate with investigators, and to national policymakers and local law enforcement agencies to monitor and enforce them, make use of Europol's practical tools and recommendations, and oversee the lawful application of investigation and surveillance techniques related to 5G.

“Von der Leyen should take a closer look at the agency's decryption platform and innovation lab for a more holistic view of 5G and the balance between freedom and security.”

¹² Van Gemert, Wil. “Update on European Cybercrime Centre (EC3) Activities.” February 2019.

¹³ Council of the European Union. “Outcome of the Council meeting. 3717th Council meeting, Justice and Home Affairs” (Council doc. 12837/19). Luxembourg, October 7 and 8, 2019, p. 19.

¹⁴ Europol. “Europol Strategy 2020+.” December 13, 2018, p. 5. Accessed January 20, 2020.

¹⁵ Monroy, Matthias. “New Technologies: Europol sets up an „Innovation Laboratory.“ October 25, 2019. Accessed January 20, 2020.

2.3 Target 3: ‘A coordinated European approach on the human and ethical implications of AI’

AI refers to “systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals”. Such systems can take the form of software or be embedded in hardware devices.¹⁶ Similarly to 5G, the technology holds great potential, with possible applications in all sectors of public and private life. To reap the benefits of smart automation and machine learning in selected processes or workflows, while fully respecting data protection and fundamental rights, the European Commission initiated a process in 2018 aimed at the adoption of a European AI strategy and a ‘human-centric’ approach in research and development. Von der Leyen intends to pursue and accelerate this process. Specifically, she wants to put forward legislation for a coordinated EU approach on the human and ethical implications. A white paper mapping out possible options is expected by February 2020.¹⁷ Europol can help her achieve this goal and reinforce the ‘trustworthiness’ of the brand ‘AI made in Europe’ in two main ways.

First, the agency can support her by facilitating the coordination of political approaches within the EU as regards the security dimension of AI. Currently, the Commission’s focus lies mainly on industry policy and the single market. Additionally, EU Member States vary greatly in their positions on AI, including on whether to focus on opportunity and innovation or precaution and risk, or whether to prioritise military and security applications or civil use. At the time of writing, only 17 Member States have adopted national strategies or are currently in the process of doing so.¹⁸

Europol could help mediate between differing national positions on the security aspects of AI. On the basis of its cross-national analyses and day-to-day business, the agency could for example identify operational and political priorities as well as disparities in domestic capabilities. This includes the identification and further development of positive applications of AI to enhance not only European cyber defence and security capabilities, but also the ability of law enforcement authorities to fight and investigate crime. Europol could also play a role in raising awareness among policymakers, practitioners and the public regarding the opportunities and risks related to AI. If it were represented in relevant working groups such as the Commission’s High-Level Expert Group on Artificial Intelligence (AI HLEG), it could flag potential areas of criminal abuse or practical obstacles that might undermine the trustworthiness of AI, and thus support the implementation of the European strategy on AI.

Secondly, Europol can help mitigate the technical and societal challenges of AI. If von der Leyen wants to achieve a coordinated, human-centric approach that can serve as a European and global norm-setter, the potential technical pitfalls and

“Europol can help mitigate the technical and societal challenges of AI.”

¹⁶ European Commission. “Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe” (COM(2018) 237 final), p. 1. Brussels, April 25, 2018.

¹⁷ European Commission. “Liste des points prévus pour figurer à l’ordre du jour des prochaines réunions de la Commission” (SEC(2020) 2324 final). Brussels, February 5, 2020.

¹⁸ Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Italy, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Spain, Sweden

malicious use of related technology must be addressed. More and more criminal actors employ AI, for example to (part-)automate the distribution of malicious contents or false information, conduct social engineering or attack digital vulnerabilities.¹⁹ Illicit AI-related activities are emerging as a key threat to European citizens and economies across all Member States, and are likely to increase in their magnitude as the technology is diffused. Addressing these challenges should surely form an essential part of an EU-level debate on the human and ethical implications of AI. In this context, Europol is already engaged in analysing and countering malicious actors and trends. It works together with a variety of public and private actors, including within the EU JHA agencies' network or bilaterally, for example with ENISA, the EU Agency for Cybersecurity.

Evidently, Europol should not be the only EU agency or actor representing the security dimension of AI technology. For aspects such as cyber resilience or the protection of critical infrastructure from malicious actors and espionage, others might be more suitable or more knowledgeable points of contact, including ENISA and eu-LISA. What Europol can offer, in contrast, is a broader criminological perspective and expertise in the fight against criminal or terrorist abuse of AI. Within its EC3, it monitors and seeks to anticipate criminal developments related to the IoT and AI. Its newly created innovation lab is also likely to deal with the topic. If funded and involved appropriately, it could even play a key role in identifying and mitigating potential abuse and threats. Europol could thus support the European Commission not only in achieving a coordinated European AI strategy, but also in connecting von der Leyen's envisioned 'Europe fit for the digital age' with a Europe that protects.

3 Von der Leyen's first 100 days and beyond: where Europol should be headed

Von der Leyen's agenda in the area of digitalisation and cyber is undeniably ambitious: handling and sharing big data, introducing joint 5G standards and developing a coordinated, human-centric approach on AI. With March 9 – the President's 100th day in office – fast approaching, the pressure is on to at least lay the groundwork for these important endeavours. This policy brief has looked into how Europol could help the Commission do just this and achieve its goals in the area of digitalisation and cyber beyond the first 100 days. Table 1 summarises the key recommendations.

¹⁹ Europol. "Internet Organised Crime Threat Assessment (IOCTA) 2019." 2019; Europol. "Do criminals dream of electric sheep? How technology shapes the future of crime and law enforcement." 2019, p. 10. Accessed January 20, 2020.

Table 1. How Europol could help von der Leyen

Improving information exchange
<p>Data availability/’need to share’</p> <ul style="list-style-type: none"> • provide lessons learned and best practices from experience with Europol databases and integrated data management, concretely in the areas of: <ul style="list-style-type: none"> • purpose-driven data processing • data protection, safety and security • act as central facilitator of information exchange among competent authorities in the area of EU police cooperation <p>Joint Cyber Unit</p> <ul style="list-style-type: none"> • provide lessons learned and best practices from experience with EC3 • act as central facilitator or coordinator among competent authorities in the area of EU police cooperation
Introducing joint standards for 5G networks
<ul style="list-style-type: none"> • add a security/law enforcement perspective • identify, anticipate and mitigate: <ul style="list-style-type: none"> • security risks and challenges (‘disruptive technologies,’ malicious use etc.) • operational challenges for law enforcement and security authorities (e.g. related to legally permissible investigation, surveillance and lawful interception) • develop central practical tools and instruments to protect 5G networks and fight malicious actors (e.g. EC3, decryption platform, innovation lab)
Adopting a coordinated European approach on the human and ethical implications of AI
<ul style="list-style-type: none"> • add a security/law enforcement perspective • add a practitioner’s perspective (public and private) by harnessing its networks (JHA agencies, regular working groups, conferences etc.) • identify cross-national operational and political priorities • identify, anticipate and mitigate: <ul style="list-style-type: none"> • security risks and challenges (‘disruptive technologies,’ malicious use etc.) • practical opportunities and applications to enhance security and law enforcement capabilities (e.g. advanced investigation techniques, crime prevention etc.)

Whether and to what extent Europol will be able to support von der Leyen in these ways ultimately hinges on the Commission itself. If the agency is to help achieve these goals over the course of the coming years, the latter must fulfil three prerequisites:

1. “A seat at the table”

Stronger involvement and regular inclusion of Europol in relevant discussions at EU level, for example on the interoperability of information systems or in respective working groups (e.g. AI HLEG) among policymakers and tech companies dealing with 5G and AI;

2. “Make it official”

Legal strengthening of Europol’s role as central hub for the exchange of criminal information and intelligence, including formal references and links in the development of regulation and legislation on new technologies, ensuring de jure access to relevant information and databases;

3. “Put its money where its mouth is”

Guarantee appropriate funding and resources for Europol and its activities under the next multiannual financial framework, including the availability of data, sufficient posts in its EC3 and relevant units (e.g. further development of the innovation lab).

In the light of rapidly unfolding developments related to digitalisation and cyber space, von der Leyen’s agenda comes at the right time. Challenges from big data and new technologies – first and foremost AI, 5G and quantum computing – will only continue to grow in the next years. Whether or not Europe will be able to keep abreast of them and truly become ‘fit for the digital age’ whilst safeguarding ethical boundaries and its citizens’ security thus also depends on what role the European Commission decides to confer on Europol in all of this.

On the same topic

- Paul-Jasper Dittrich
Data Sharing: A European Challenge?
Jacques Delors Centre, Policy Brief, February 2020.
- Paul-Jasper Dittrich
In 2020, France and Germany must take AI cooperation to the next level
Jacques Delors Centre, Policy Position, December 2019.
- Dr. Nicole Koenig
The ‚geopolitical‘ European Commission and its pitfalls
Jacques Delors Centre, Policy Brief, December 2019.
- Franca König
What’s wrong with EU information systems and how to fix it
Jacques Delors Institute – Berlin, Policy Brief, September 2018.

Hertie School gGmbH • Chairman of the Supervisory Board: Bernd Knobloch •
Chairman of the Board of Trustees: Frank Mattern • Academic Director:
Prof. Dr. Henrik Enderlein • Managing Director: Dr. Axel Baisch • Registered Office:
Berlin • Trade Register: Local Court, Berlin-Charlottenburg HRB 97018 B •
Hertie School – founded and supported by the non-profit Hertie Foundation
Image © Johannes Plenio, Source: Pixabay.