

SYNTHETIC REALITY & DEEP FAKES IMPACT ON POLICE WORK

October 2021



Best Practices | Co-Creation | Research

European Network of
Law Enforcement
Technology Services



INTRODUCTION

This document was prepared by Manon den Dunnon from the National Police of the Netherlands. Manon is a member of the Internet Investigation Technology Interest Group and in June of 2021 delivered a presentation and training to co-members on the complexities and nuances of various Deep Fakes and Synthetic Media. The report is a working document to capture some of the current state-of-the-art, and it is a useful tool for LEAs and the research community to familiarise themselves with synthetic media in its various forms and understand the associated risks.

Status as of June 2021 - feedback is encouraged.

ABOUT ENLETS

The European Network of Law Enforcement Agencies (ENLETS) brings together 29 members from across Europe to action shared priorities. The group frequently meets to discuss relevant topics related to technology and associated matters. Through National Contact Points, the group exchanges information and updates on the latest issues concerning the strategic points the network is focusing on at a given time.

ENLETS works by sharing best practices on a broad level, engaging on mutual priorities and stimulating future research. The environment promotes collaboration and fosters a supportive network working to help each other through current challenges.

At the Technology Interest Group (TIG) level, best practices sit at the centre and ideas and insights help foster progress across Europe. The groups share use cases, recent projects and challenges. A secure chat application - Stashcat - is widely used between meetings to support the exchange of good practices and valuable materials that support the efforts of each group.

contact@enlets.eu

enlets.eu

AUTHOR

Manon den Dunnen is working at the Dutch National Police as a strategic specialist on digital transformation.

She monitors trends in technology, their effect on society and the possible consequences for the work and role of the police. Manon's main focus now is on raising awareness about the consequences of digitisation for the constitutional values, especially in the context of;



1. Synthetic media, deep fakes and how to and assign value and trust in a computer-generated world
2. The Internet of Everything (Things) including the intersections with social innovation, AI, Smart Cities and Cybersecurity.

Next to showing potential, Manon creates awareness about the threats and ways to deal with them.

TABLE OF CONTENTS

1. Synthetic media & deep fakes
2. Current state of synthetic media
3. Impact on Law Enforcement
4. Police approach to synthetic media
5. Annex 1 - Disinformation

1. SYNTHETIC MEDIA & DEEP FAKES

Synthetic media can be defined as media generated or manipulated with Artificial Intelligence (AI).

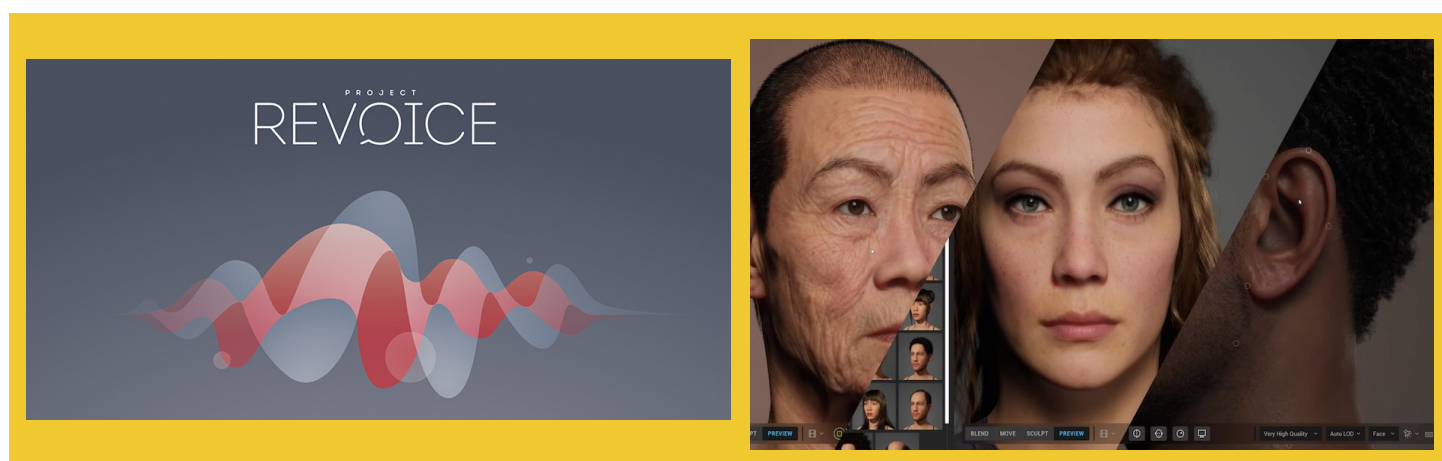
For example, images, faces, sound, voices, texts or even moving people. But it's not limited to that, every biometric characteristic can be synthetically manipulated or cloned, just like any signal that is put into sensing applications and automated decision-making, in fact, all digital information and signals.

In this document, we limit ourselves to image, audio, and text.

Within the domain of synthetic media, there is a subgroup called Deepfakes. The term deep fake dates from 2017, when a user with that name on the social media platform Reddit shared nude photos with celebrities' faces (so-called face swaps).

every biometric characteristic can be synthetically manipulated or cloned

Originally, the term deep fakes referred to malicious Faces Swaps and StyleGANs, specific forms of AI, which uses existing images as training material to generate new unique faces. At the moment, however, the term deep fake is used for everything, including for non-existent persons generated with (other forms of) AI to be used in games. And also for positive applications, such as cloning the voice of someone with ALS who's losing his/her voice.



1.1 CONCERN ABOUT MALICIOUS SYNTHETIC MEDIA

The growing concern about synthetic media and deep fakes in particular stems from the increased accessibility and that

everyone can now create synthetic media themselves or use one of the many deep fakes-as-a-service platforms.



And when you combine synthetic media with the ability to fully automate the targeting of people, in small groups or individually, on social media, the impact is huge- especially given our deep-seated tendency to believe what we see/hear for ourselves. Next to crime, synthetic media can also be applied in the context of disinformation to add a false sense of authenticity. Disinformation is beyond the scope of this report, but some context is added in Appendix 1.

What worries people most, given the impact on trust, is the so-called liar's dividend; being able to claim with impunity that something real is fake. You see this phenomenon more and more, also among politicians. But when real evidence can be dismissed easily as deepfake, it affects trust in journalists, police and judges, thereby threatening the fundamentals of our democracy.

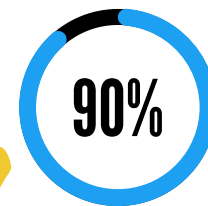
For the police, this erosion of trust means that more evidence will be required and that we need to be even more transparent and proactive about the sources and possible trade-offs with regard to the evidence.

Deepfake prices	
Service	Price
Deepfake videos	From US\$50
Deepfake still images	From US\$2.50 each
Software to create deepfakes	From US\$25

1.2 EVERYTHING WILL BE SYNTHETIC

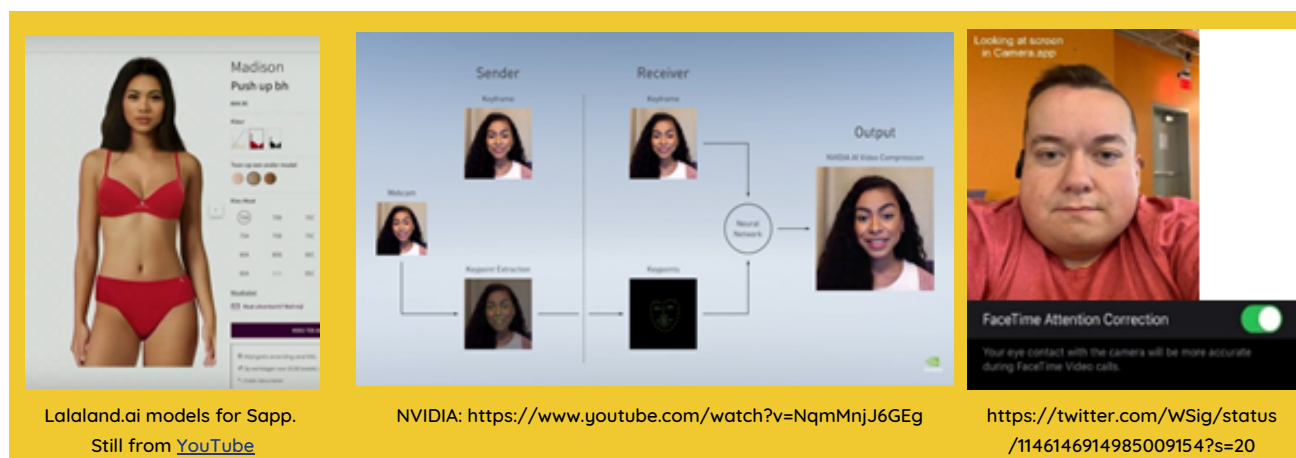
We are now talking about deliberate deception, but the question of what is fake and what is real will be given a different meaning in the coming years. This has to do with the fact that more and more online content is generated synthetically, “fake” by definition. This happens visibly in movies, games and on websites, for example with fake synthetic models to allow you to choose products to suit your skin colour, but also, behind the scenes, to improve service, for instance, in video conferencing.

To save bandwidth and give you the sensation that you are talking to each other, audio and image on the receiving end are increasingly artificially generated and/or manipulated.



Experts believe that within 6 years, 90% of the online content will be synthetic.

This process has been going on for some time, for example in phones. This occurred when people wanted to take photos and videos of the orange sky during the great bushfires in California. According to the AI built into many phones, the sky could not be that orange, so the color was synthetically adjusted to grey...



Deep fake models, deep fake skies generated by our phones and synthesized video conferencing - with all, there is no malicious intent, but it does affect our perception and thus we need to adapt our methods of establishing the facts, the truth of what happened (the truth of what is real).

Before going into the implications for Law Enforcement, the next chapter will first give an overview of current capabilities in video, audio and text synthesis, as well as detection.

2. CURRENT STATE OF SYNTHETIC MEDIA

Initially, the technology was used in the ‘graphic processing industry’ intended for analysing large amounts of visual data to make predictions. This has led to great advances in, for example, weather forecasting, cancer detection and safe autonomous navigation by self-driving vehicles. In this document, we limit ourselves to image, audio and text synthesis.

2.1 IMAGE SYNTHESIS

In recent years, we have seen the use of synthetically generated images also increase significantly outside the science, industry and medical sectors. Well-known examples are the revival of already deceased people, such as [Dali](#) who welcomes the visitors of his museum, but also “ordinary” people in the context of [mourning](#).

Living people are also cloned, such as [this employee](#) of an investment bank, to be able to provide more customers with investment advice. And applications to protect vulnerable groups such as in the documentary [Welcome to Chechnya](#) or for educational purposes such as David Beckham’s [malaria awareness](#) video. In addition, there are completely new synthetic characters, such as [newsreaders](#) who report the news 24/7 without ever getting tired.



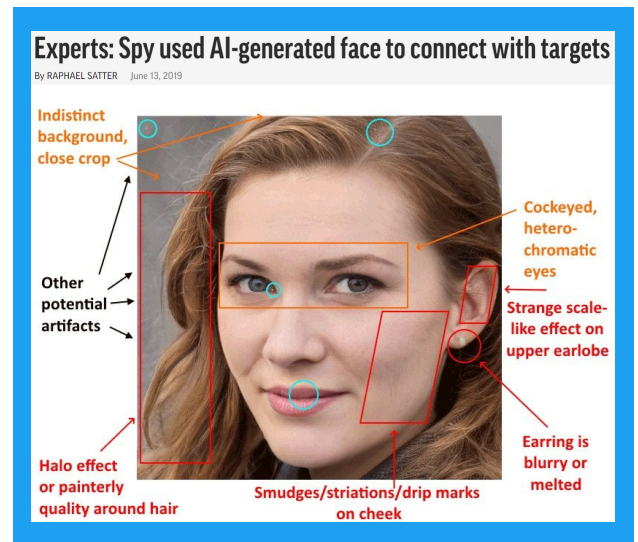
Since Corona, synthetic images are increasingly being used in advertising and [training](#) (in Virtual Reality).

(Revenge) porn is still the most common malicious use of synthetic images. In 2020 a Telegram [bot](#) was discovered that allows you to upload a photograph of a random person, after which you get a manufactured pornographic image of the same person.

But more and more you see news reports about the use of deep-fake images for disinformation, scams, activism and even espionage.

Moreover, the fictional Katie Jones, with a deep-fake profile photo on LinkedIn, managed to build a network within the highest echelons in Washington.

A Dutch example is the [covert influencing campaign](#) in which hundreds of fake Indonesian accounts were acting on Facebook and Twitter – also in Dutch – against Papua independence activists.



Deep fake profile photos were also used. You can easily obtain these from the website [thispersondoesnotexist](#).



For regular use of stock photos, websites have emerged where you can generate customized people:



With deepfake technology existing identities can also be counterfeited, to be used for identity theft, or to fool access systems.

FAKE



There are many tools to manipulate images and videos. Already in 2018, German activists succeeded in applying for a [passport with a photo](#) in which two faces were merged. The tools are also increasingly used in the context of disinformation. Of course, this doesn't always require deep fake technology. Cheap fakes, i.e. manually manipulated images and videos, for example with Photoshop, are still the most common.

2.2 AUDIO SYNTHESIS

With sufficient training material from an existing voice, you can generate a synthetic clone of this voice. This synthetic audio can, for example, be used to give people with the disease ALS their own voice back. [Veritone](#) just launched a platform for famous people where they can clone and licence their voices. This way their voice can be used to create audiobooks or radio commercials at any time independent of its owner.

You use text as an input to make a synthetic voice say things. This way you can also easily adapt existing statements (audio fragments). Another interesting application is so-called image-to-audio synthesis. Based on machine learning, the AutoFoley program recognises what's going on in a video clip, after which it automatically adds the right sound effects to it.



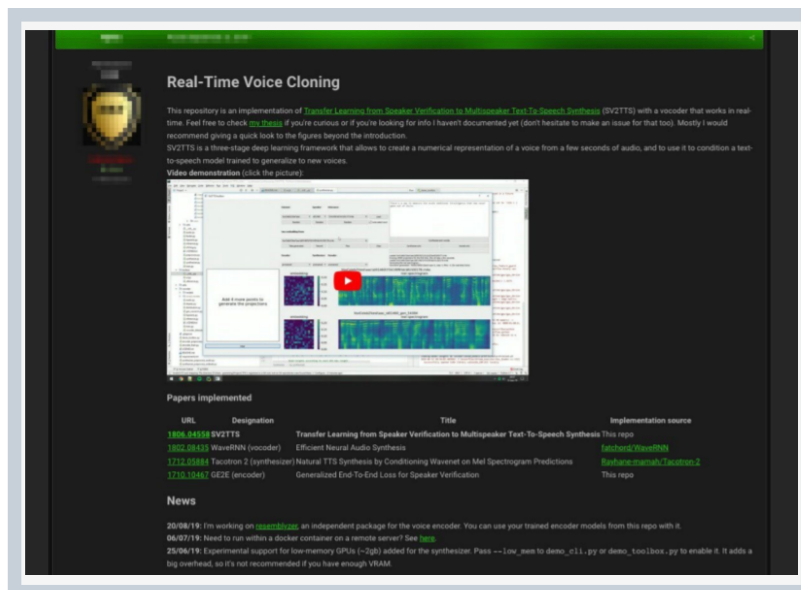
Synthetic voices used to be monotone, but Sonantic has succeeded in making AI express emotions in a realistic way.

There are few examples where synthetic audio is used maliciously. For example, a British energy company was scammed with a telephone call for EUR 243.000,-. The scammers used software that imitated the voice of the boss of their German parent company. The voice of an ex-boss of Europol was also replicated to steal EUR 10,000.

The risk of criminal applications with synthetic audio is expected to increase significantly in the coming years, partly due to the growth in the use of voice assistants.

Both Google and Amazon are working on biometric voice recognition to make their voice assistants sufficiently safe to do banking business, for example.

This development is already being undermined by the emergence of tools to make deep-fake voice clones and the trend in which more and more products and also the environment are made 'smart' within the framework of the Internet-of-Things. Microphones and speakers are increasingly being added. Via hacked speakers, devices can be controlled, but Alexa can also be activated for banking or ordering.



Online is advertised with real-time voice-cloning, only an audio recording of 5sec is required. Source Europol

Other examples of criminal applications can be found in this [report by Europol](#). Considering the tendency of our brain to believe what we see and hear ourselves, a major threat stems from the combination of different forms of synthetic media. When criminals combine sending text messages via e-mail or WhatsApp with audio calls, it becomes very difficult to recognize that you are being scammed.

2.3 TEXT SYNTHESIS

Text synthesis is in full development. In early 2020, GPT-3 was launched, a new language model for text generation. After that Google and China followed with alternative [models](#). The systems are trained with all the texts they were able to extract from the internet, so it can now generate appropriate new text based on the input text. Unfortunately, considering that the training material, our internet, is anything but neutral, the use of such tools poses many risks in terms of discrimination[1].

But text synthesis also offers interesting opportunities. By training it specifically on the material of a specific person, you can generate texts featuring the same choice of words and way of “speaking”. This way you can generate new books from deceased writers. Other applications are the generation of texts with a high degree of predictability, such as contracts, quotations, legal documents, manuals, or the highlighting of sentences that stand out in documents consisting of hundreds of pages.

In theory, text synthesis, especially in an administrative-intensive organisation like the police, can offer many opportunities. However, research by the AI Lab of the Dutch Police shows that it is still too early for deployment.

Thanks to new language models, it has become much easier to analyze texts and generate variations in large volumes. This can be used to guess passwords, and automate social engineering in many forms of scams and extortion.

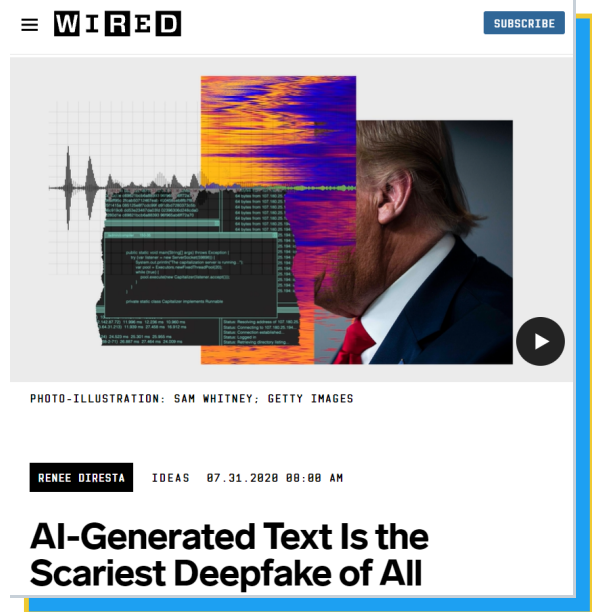
Wired published an article warning that it might also be used [to create a web of lies](#), concealed as regular conversations on social media. This could also undermine online debate.

[1] Nog toevoegen links naar discriminatie voorbeelden

[2] The thesis ‘Hybrid methods for data-to-text generation’ by Gaël De Léséleuc De Kérourara, written under the supervision of colleague Dr. Bas Testerink of the police AI lab.

At the moment it is still laborious to create the programs behind fake accounts (so-called bots) and they are often easily detectable. Soon AI will be able to generate authentic-looking content on any subject. After which other AI will read it, formulate and publish replies, after which they respond to each other again.

Due to the enormous artificial engagement created, there is a real risk that the information created by AI will be prioritized in news feeds and timelines and thus, in our (global) information system (see also the appendix on disinformation).



This means that, on the one hand, it becomes increasingly difficult to reach people with your own message, and on the other hand it becomes more difficult to find correct information as a human being.

Technologies combined

In 2020 [Dall-e](#) was published, specifically trained to generate images from a descriptive text (text-to-image synthesis). alongside you see images generated from the input: armchair in the shape of an avocado.



Also interesting is this example of AI technology to [analyse and adapt](#) recordings of existing events, in this case, a broadcast of a tennis match.

It has great potential for training, debriefings but also to visualize ‘what if’ scenarios. Obviously, this also presents risks in the context of disinformation.

2.4 DETECTION

Unfortunately, there are **no good tools** (yet) for the automated detection of synthetic media such as deep fakes. On top of that, the available tools do not detect so-called cheap fakes (like photoshopped) since they focus only on images generated with specific forms of AI.

However, if you are aware of their limitations, using a tool that scores 65% can still have added value. Examples of free tools you can try can be found [here](#).

In the long run, detection tools are not the solution. First of all, because the same detectors can be used to test and create better deep fakes. As a result, deep fakes are expected to become so good that detection is no longer possible. Despite this, major tech companies such as [Facebook](#) and [Microsoft](#), as well as governments (USA) invest a lot in developing new forms of detection.

It is relevant to follow these developments because they will also increasingly anticipate the trend in which more and more content such as images, audio and text are generated synthetically.

They have to as, within 6 years, more than 90 % of the online content is expected to be synthetic. As a result, a detector for deep fakes will continuously send alerts.

3. IMPACT ON LAW ENFORCEMENT

As the police is an information-led organisation, every aspect of policing is affected by synthetic media. Synthetic media offers opportunities and poses threats in the context of crime, information management, truth-finding and trust as will be described in this chapter.

3.1 OPPORTUNITIES

The AI lab of the Dutch police conducts applied scientific research into the possibilities of synthetic media. The identified possibilities will then be tested in operational practice.

Short-term opportunities are in the context of:

- Chatbots for customer and employee contact;
- Creation of large test databases for training our own AI to help us detect objects or actions in photo, video and audio;
- Information sharing with the general public customized to people's own language, by trusted (synthesized) persons;

In the medium term, there are opportunities for:

- Tactical deployment of synthetic media within criminal investigations and systematic collection of information. In this context ethical considerations should be taken into account.
- New possibilities for the protection of witnesses and (covert) police colleagues;
- Training, scenarios, debriefing, or trauma processing.

3.2 CRIME

As with any new technology, synthetic media can also be applied in a harmful way. Examples of this have already been mentioned in the previous chapter.

In the 2020 AI-enabled future crime report, the imitation of people in images and sound was considered the biggest threat. More recent insights as shared by Wired and Europol show that the potential damage of text synthesis could be even bigger, especially when combined with audio and images.

But also control and access systems are impacted as one can train and improve synthetic clones endlessly against detectors. Research from Sensity.AI showed that several online facial identification systems, in use by banks, are vulnerable to real-time face-swapping. And in 2020 McAfee managed to create an image that looks like person A to humans, but is identified as person B by the computer (face recognition systems).



The malicious applications of synthetic media, especially in the context of identity, extortion and fraud are endless. Because of the accessibility, scalability and increasing effectiveness we can expect an exponential rise in related crimes.

And as the report of Europol points out, we still have to come up with answers, but a joint effort in creating awareness and countermeasures will certainly help!

3.3 INFORMATION MANAGEMENT

Information is key to every aspect of our work. The fact that ever more information is generated or manipulated with AI provides a new perspective, regardless of whether it is malicious or not. As communication and reporting are increasingly digitized, important aspects of non-verbal communication that we normally take into account could be manipulated without both ends knowing.

Areas that are affected:

- **Information that partners provide**

It is very important to be able to verify at all times the integrity and authenticity of the information we use. When obtained from third parties, there is no insight into how the information came about. An open conversation could provide more insights into the vulnerabilities and how to deal with them. An example is a current process of applying for identity documents; people can still submit a photo made by themselves.

- **Information generated within/by the police**

Also, evidence that we ourselves generate, such as observation photos, can be dismissed as “fake”. This also happens in journalism. That is why the industry is already working on ways of proving the origin (provenance) of the information.

- **Information collected by the police (e.g. social media, interception systems)**

How do you assess and substantiate the value of the information in context?

- **Information provided by the public (witnesses, declarant)**

If you don't know if the information is manipulated, how to decide who is the suspect? The person depicted in the video/ photo or the one who made or provided the video/photo?

- **Agenda setting (prioritizing)**

An increase in (artificial) online ‘storms’ that constantly ask for attention and response is a real risk, this leaves less time for attention to real priorities. The assessment of whether or not to respond is complex because it can also add to the ‘storm’.

And even if the information is not real, the police may still have to act on the social unrest that certain information causes.

We will have to adapt our way of working to the increasing uncertainty and manipulation possibilities. For instance a greater commitment to verifying information, working with hypotheses and scenarios, but also raising awareness of the imprint that we and witnesses may experience. More on this is described in the Annex on disinformation.



Oregon wildfires: False Oregon fire rumours 'inundate' officers

A deluge of misinformation about fires in Oregon prompted local officials to debunk rumours.

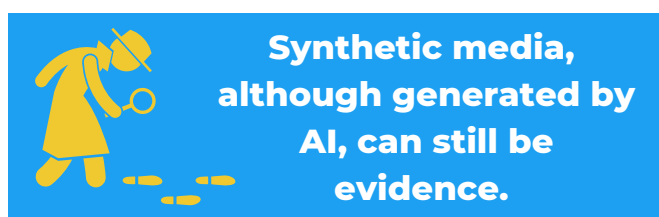
Within the police, but also at the Prosecutor's Office, the magistracy, and all partners in public order and safety, including the criminal justice chain, must build knowledge on this phenomenon in order to ask the right questions and to be able to interpret information in context.

Automated recognition of synthetic media is not effective but could contribute in a clearly defined context. Sometimes synthetic material can be directly punishable, think of virtual child abuse material. Yet there is an interest in being able to distinguish in a collection of millions of images as to pick out the ‘certainly real’ children. This can save time and effort that can now be used to find and free the real children.

3.4 TRUTH FINDING

The so-called Liar’s dividend also affects trust in information and evidence provided by the police. Any digital evidence could be questioned.

But not only because of the Liar’s dividend, also from the perspective of truth-finding, it is necessary that we look at digital information from multiple perspectives and sources to understand and substantiate the evidential value in a transparent way.



There will soon be both completely new AI-generated characters and so-called Digital Twins of physical persons, who lead their own autonomous lives (deviating from the original person) in which they generate real traces/information.

The question is to whom these traces can be attributed and who is accountable for the consequences. For example, synthetic newsreaders are clearly part of an organisation that is accountable. Soon, however, there will also be self-learning autonomous systems and personas without a clear owner or maker.

It is still unclear what the new meaning of fake and real will be, but it is about the contribution to truth-finding in a certain context, the evidential value. Clues can be found by looking at the context; maker, importance, motive, purpose, metadata and by backtracking digital traces to the software used.[3]

This requires multidisciplinary research, such as in the field of digital forensic expertise, OSINT, Humint (information from human sources) and both common and domain knowledge. Validation by several independent parties outside the police can also contribute. For example, the platform where the information was uploaded/shared, the supplier of the device or software, etc.

A number of questions need further examination:

1. What new standards and procedures (accreditations, audits, oversight) are necessary to give unambiguous value to evidence in the context of truth-finding and to substantiate the evidence in a transparent way.
2. More often evidence may need to be assessed in a scientific way by working with hypotheses and probability rates. The police are not experts in this area, and cannot report scientifically because they are party to the trial. Forensic Investigations are regulated in such a way that the police do the technical research and the NFI (Dutch Forensic Institute) the scientific research. This means quite a bit for the capacity availability of parties such as the Forensic Institute. And as with DNA, officers, lawyers and judges will have to learn to deal with likelihood ratios (LR) for the evidence whose authenticity is under discussion.

[3] You can replicate someone else but also create something. Prof Eiben of the Vrije Universiteit already developed self-propagating robots in 2016. intended for deep-sea research or on Mars, in order to adapt themselves autonomously to the conditions on the ground.

4. POLICE APPROACH TO SYNTHETIC MEDIA

We propose the following action lines:

- Awareness
- Organisation
- Research & collaboration

4.1 AWARENESS

This is the most urgent line of action. Every police officer must be aware of the possibilities of synthetic media, the effect on their own work and how to deal with it.

This can be done via webinars, presentations, workshops, training material and input for the briefing [4]. By initiating conversations, we can also explore impact, opportunities and possible actions we have not foreseen.

As awareness is just as important for other organisations involved in public order and safety, a common awareness campaign could be created in collaboration with partners.

Creating awareness among the general public is also recommended. Making citizens more resilient seems to be the best way to combat disinformation and the erosion of trust. The government is in charge of this, but the police can contribute and strengthen the initiatives by referring to them.

[4] Appealing examples of awareness campaigns without linking with police practice, deepfakes: <https://www.spotdeepfakes.org/>; disinformation: <https://harmonysquare.game/en>

4.2 ORGANISATION

Within the Dutch Police, a multidisciplinary community is already being built around the theme of deep fakes and synthetic media. Some police teams are also working out the impact on their working practices. For each process we should:

- assess the vulnerability of procedures and information systems to synthetic media (e. g. online declaration, sensing applications)
- Identify what (supporting) knowledge, skills and resources are needed.

The developments described clearly require an adjustment in the working method.

The Digital Investigation Program has included the following for its 2022 agenda:

1. Tools for synthetic and manipulated media.

Design a toolbox that can contribute to detect (synthetic) manipulations in image and sound.

2. Quality and evidential value of digital information.

How to explain and substantiate in a transparent way the quality and evidential value of digital information. Defining the adjustments needed in processes, methods and standards.

Collaboration with partners, but also public and private cooperation is necessary on both subjects.

4.3 RESEARCH & COLLABORATION

- Create a multidisciplinary monitor for the malicious use of synthetic media.
- Expansion of and deepening on specific expertise, such as audio, text synthesis and knowledge of embedded AI in tools/devices used.
- Comparative research into the applicability of available tools for the detection of (synthetic) manipulated images, audio and text.
- Experiments and research into the possibilities for tactical deployment of synthetically generated persons/objects, with particular attention to ethical aspects.

- Research into possibilities to authenticate data generated by ourselves. Internationally, a lot of [standardisation](#) has already been done. For the police, Witness.org's involvement is valuable, they support citizen journalism and therefore also take into account the balance between proof of origin versus maintaining the anonymity of the maker.
- Research into the consequences for Sensing and possibilities to define safeguards for existing and new sensors (how to authenticate signals).
- At the European level, the dialogue with the major tech platforms has to intensify, as that is where malicious synthetic media often emerge.

ANNEX 1 - DISINFORMATION

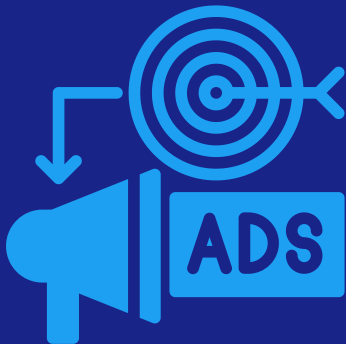
Disinformation involves the deliberate dissemination of misleading information. The functioning of our brain and the workings of many well-known social media platforms and search engines empower both the rapid dissemination and the impact of disinformation. The possibilities of synthetic media, such as deep fakes, accelerate and strengthen this process.

A1.1 MECHANISMS BEHIND SOCIAL MEDIA

Commitment

Often disinformation is shared in such a way that it evokes emotions and the urge to do something, if only a like, share, or retweet. This means that people are paying attention to the message. This so-called engagement is an important indicator for prioritizing a message in news feeds, timelines and search engines, as it implies that you as well will be likely to click on it. Providers of social media platforms and search engines have an interest in keeping you on their platform for as long as possible. The longer you stay, the more ads they can show you, as well as the more data they can collect about you(r) behaviour.

They can sell this data, but they also use it to create a profile of you, which allows them to provide you with even better (personalized) services and information, that hopefully keeps you on their platform or return faster.



A consequence is that when you look for something on Google, watch trending topics on Twitter, or get news presented in your timeline on Facebook, it will be different from any other person.

Based on your characteristics and previous behaviour, you get the information the system thinks is the best fit to what it assumes you are looking for. This is how you end up in a so-called personal filter or information bubble.

To keep you hooked, the system also tries to offer similar new information prioritizing headlines that evoke your curiosity or stimulate your emotions to keep you clicking on. This can result in the information you see getting more and more extreme. The Netflix film, *The Social Dilemma*, gives more insights on this topic.

Majority Illusion

Another aspect is that the underlying structure of social networks can ensure that behaviour or opinion that is rare worldwide can be systematically over-represented in a local environment when certain key figures share it. [Research](#) shows that these are not the influencers with the most followers. So if you can influence the right people in a network, you can create this so-called “majority illusion“. In doing so, it seems that everyone shares a certain opinion, which makes you feel inclined to go along with it. This is also used by so-called ‘troll bots’ that feed large amounts of automated fakes into discussions.

Illusory truth

In this context, the concept of illusory truth (imprint) is also important, this describes our tendency to believe false information when we are repeatedly exposed to it. This has to do with our brains trusting things that we hear and see ourselves. Even though we know that something is wrong, we (unconsciously) still believe in it because we encounter it so often. [5]

Consequences

In their own information bubbles, people are not exposed to any nuance or debunking. And if you are exposed to apparent injustice long enough, without seeing anyone intervene, you can be prompted to take action yourself. Examples include the 5G masts that were set on fire, the man in the Pizzagate, who went to free children from a non-existing basement under a pizzeria, and the recent storming of the Capitol in America.



[5] So never share or like disinformation, not even to express your disapproval, you only contribute to the illusory truth and engagement.

A1.2 DEALING WITH DISINFORMATION

The detection of disinformation is complex. First of all, the question arises who determines that it is disinformation. Internationally the question “who checks the fact-checkers” continues to pop up. In addition, people and politicians in the public domain have a certain freedom to debunk untruths.

The question is also what the role of the police should be. The disinformation about the relationship between 5G and Covid most likely led to arson at telecom masts and did impact police work. But did the police have a proactive/preventive role there, or is it the responsibility of the owners of the telecom-towers, or the platforms on which the disinformation was shared?



There have been several international studies on the best approach to disinformation. Raising awareness seems to be the most effective. The (repetition of the) denial of information is also widely recommended, but studies show that there are differences of opinion about the effectiveness. This is related to the context and to who is the one debunking.

Crowdsourcing

The “crowd” can play an important role in timely alerting for disinformation, even when disinformation circulates in closed sources. When it starts to get out of hand there is always someone sharing it outside the group. By being well connected both online and offline! Besides, by intensifying the monitoring of open sources (OSINT), it is possible to address and limit the impact of disinformation in a police context.

Sharing signals within the OSINT community and checking in with related key figures outside our organisation, can also improve the speed and quality of interpretation.

It matters who contradicts certain disinformation. Networked communication can contribute to the effectiveness of neutralising disinformation.

What new partners and existing partners, independent of the police, do we recognise in this context?



This report contains the status quo of June 2021.
If you want to be updated on further developments, please
share your email address with:
Manon.den.dunnen@politie.nl
Contact@enlets.eu

Contact Details

contact@enlets.eu
enlets.eu

ENLETS Secretariat

Slowackiego 17/11 Street
60-822 Poznań | Poland
+48 61 663 02 21



This project has received funding from the European Union's Internal Security Fund - Police Programme under Grant Agreement no 814756

