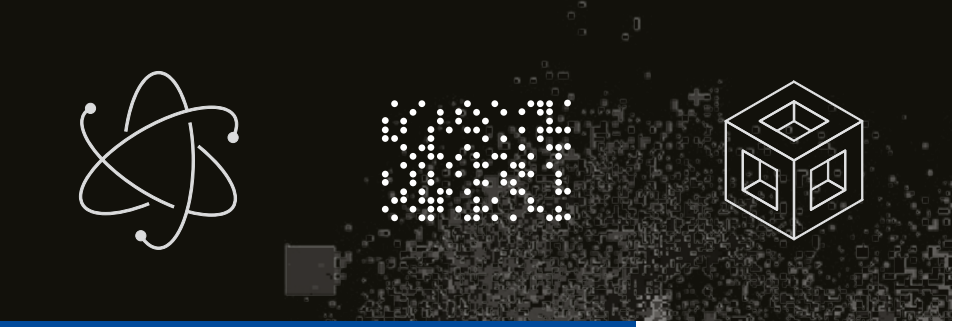
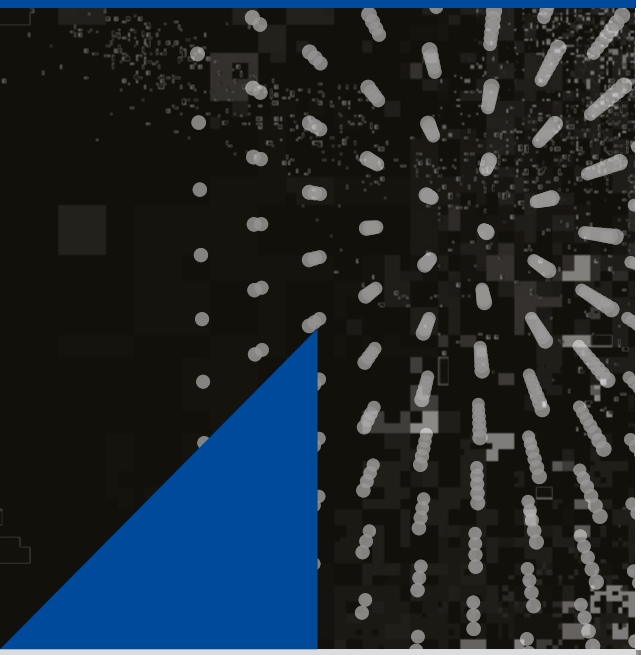
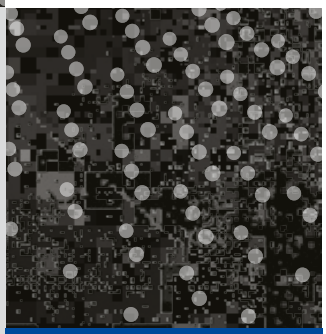


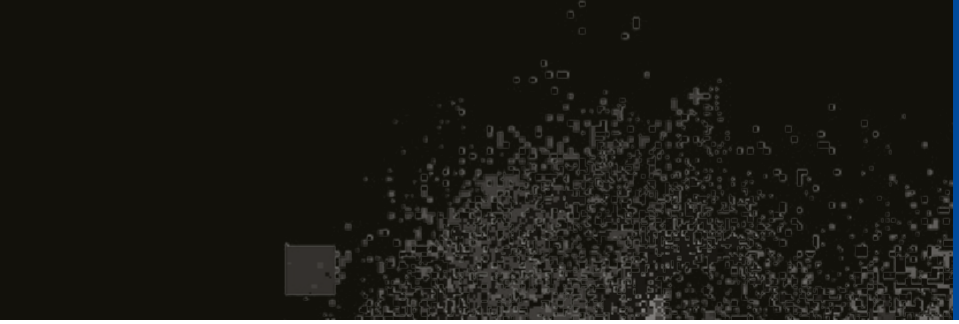
THE MOTIVATIONS FOR CYBER-ATTACKS ARE INCREASINGLY STATE-ALIGNED AND IDEOLOGICALLY MOTIVATED.



Cyber-attacks

Cyber-attacks targeting critical infrastructure, governments, businesses and private citizens are highly threatening and impactful due to a broadening attack-surface, and data theft acquiring a central role. Lines are further blurring between profit-oriented and ideologically-motivated cyber-attacks, and the cybercrime landscape is further fragmenting. AI will continue to leverage more sophisticated and scalable cyber-attacks that will even more target data than is already the case today. Cyber-attacks have a wide impact spectrum, including financial consequences, loss of personal data and eroding sense of security.





Data is a central commodity in the malware threat landscape.

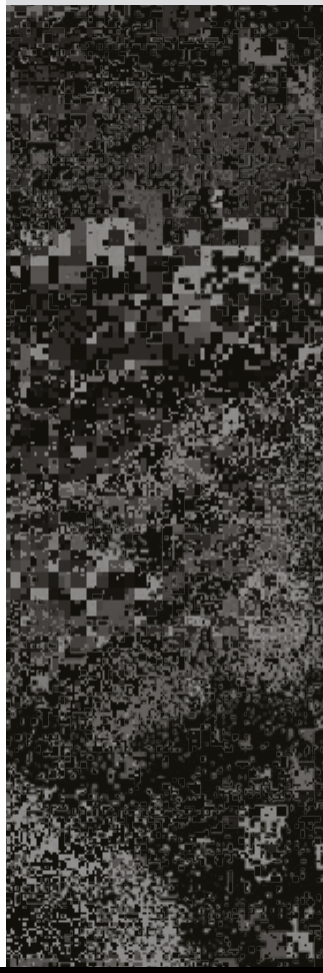
Broadening attack-surface in which data are key, further enhanced by AI technologies

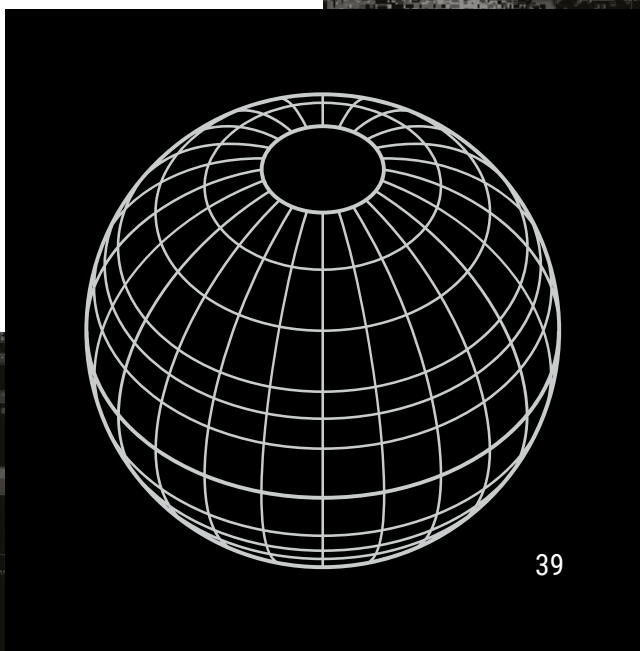
Crime is nurtured online. The number of cyber-attacks against public and private entities has increased[9], and this trend is expected to continue in the future. The rapid digitalisation of everyday life has resulted in the increased complexity of most digital infrastructures. Combined with the speed of transition and the insufficient digital literacy of the broader user base, this has left more systems exposed and vulnerable to cyber-attacks. The increase in cyber-attacks is further driven by the development of more sophisticated tools and techniques available in the Cybercrime-as-a-Service (CaaS) market.

In today's complex digital infrastructures, cyber-attacks increasingly exploit their vulnerabilities.

There is an increase in politically motivated cyber-attacks against critical infrastructure and public institutions, originating from Russia and countries in its sphere of influence.

Politically motivated cyber-attacks demonstrate precisely how the three elements of the DNA of crime work in tandem, completely changing the criminal landscape. Cyber-attacks are increasingly directed by networks and agents based outside EU external borders. Digital platforms and tools provide the perfect breeding ground for illicit activities. And cutting-edge technologies are making attacks faster, smarter, and more devastating than ever.





In order to gain entry to systems, criminal actors exploit zero-day vulnerabilities[10], Common Vulnerability Exposures[11], misconfigurations in public-facing infrastructure and leverage vulnerabilities that have been disclosed but not patched. The growing reliance on different digital service providers (e.g. virtual privacy networks (VPN), cloud, e-mail, and software service providers) increases the risk of supply-chain attacks, where a victim's system is breached by compromising a trusted third party. Social engineering methods and phishing kits[12] are widely available on the dark web. Criminals also use phishing-as-a-service to distribute emails containing malicious macros and files to steal login credentials.

CASE EXAMPLE – Notorious ransomware group dismantled[13]

In February 2024, law enforcement from 10 countries disrupted the LockBit ransomware, causing billions of euros worth of damage. It first emerged at the end of 2019, and in 2022 it became the most deployed ransomware variant across the world. The group is a 'ransomware-as-a-service' operation, meaning that a core team creates its malware and runs its website, while licensing out its code to affiliates who launch attacks. LockBit's attack presence is seen globally, with hundreds of affiliates recruited to conduct ransomware operations using LockBit tools and infrastructure. Ransom payments were divided between the LockBit core team and the affiliates, who received on average three-quarters of the ransom payments collected.

The ransomware group is also infamous for experimenting with new methods for pressuring their victims into paying ransoms. Triple extortion is one such method which includes the traditional methods of encrypting the victim's data and threatening to leak it, but also incorporates Distributed Denial-of-Service (DDoS) attacks as an additional layer of pressure.

Droppers are similarly used to allow criminals to evade and deactivate security measures and deploy additional harmful programs. They have become more effective over the past few years with the newer variants being able to evade dynamic detection, and deploy sophisticated obfuscation methods[14]. Droppers are most commonly spread through phishing campaigns.

Access to compromised systems has become a commodity in the CaaS economy, with access to compromised systems sold in bulk or auctioned on dark web forums. Compromised victims can be subjected to several simultaneous or consecutive cyber-attacks.

The crime-as-a-service economy enables different forms of cyber-attacks, including dark web market forums selling stolen data, intrusion services as well as criminal hosting and proxy providers.

Malware-based cyber-attacks[15], especially ransomware[16] and info-stealers[17], continue to be a prominent threat with data acquiring a central role[18]. Stolen credentials can be used to gain unauthorised access to digital assets, including sensitive information, that can be stolen and held for ransom. Data stolen with the use of info-stealers can be used for various cyber-attacks and online fraud schemes.

Data is a central commodity in the malware threat landscape - used for carrying out attacks, as target, and as by-product of attacks.

Within ransomware attacks, the tactic of threatening to publish exfiltrated sensitive information has become a key coercion method. There has been a shift from mass distribution of ransomware (e.g. through phishing campaigns) to more targeted attacks against private industries, critical infrastructure, healthcare, and other public institutions[19]. In recent years, targeted ransomware attacks against small and medium-sized businesses have also become more common. There has been a growing number of supply chain attacks[20]. Leaks of source codes, combined with rapidly improving AI tools, have also accelerated the development of new ransomware variants.

Crime is accelerated by technology and AI. As AI technologies improve, they will start playing an increasingly important role in criminals' tactics, techniques and procedures. They can be used for hyper-realistic social engineering attacks using deepfakes or voice alteration, or can be taught to impersonate the mannerisms, writing style and background knowledge of a person. AI can also be used to improve and automate criminal processes like finding new exploitable vulnerabilities, triaging stolen information or automating ransom negotiations or different forms of online fraud schemes, increasing the scale of attacks. Data theft will play an increasingly central role in different forms of cyber-attacks, given its importance in AI-driven attacks.

Hybrid and traditional cybercrime actors will increasingly be intertwined, with state-sponsored actors masking themselves as cybercriminals to conceal their origin and real disruption motives. Overall, it is expected that ransomware, data theft extortion and multifaceted extortion – employing complex, multi-layered tactics to maximise pressure on victims and increase the likelihood of payment – will become the most disruptive crime globally, both in volume and impact. An increased availability of CaaS, with the support of generative AI technologies, will lead to more attacks and potentially increase their efficiency. An increased use of automated tools has also been observed, for instance, to distribute malware on a large scale and adapt payloads to bypass traditional security measures. AI-generated content is also being used in phishing campaigns.

Cyber-attacks leveraged by hybrid threat actors may take further prominence against the backdrop of a shifting global geo-political balance.

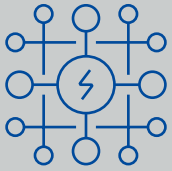
Criminal engagement driven by financial, ideological, and service provision motives

Financial motivation remains the primary driver for most cyber-attacks. Ideological motivations or service provision to hybrid threat actors in the context of hybrid threats are also common. Criminal networks engaged in cyber-attacks are present and active in a number of different countries, both in terms of the physical location of their members and the jurisdictions where they carry out their activities. Cybercriminals continuously improve their intrusion and attack techniques and countermeasures to stay ahead of evolving security solutions.

Independent ransomware groups or malware-as-a-service providers often function with a core group surrounded by a network of individuals (e.g. affiliates, other service providers). The threat actors behind these groups are technically advanced and capable of carrying out sophisticated, wide-scale attacks. The ransomware landscape has become more fragmented due to international law enforcement actions and internal disputes, forcing ransomware operations to disperse or rename themselves to cover their tracks.

The cybercrime landscape has become more fragmented, with shorter life-spans for and splintering of markets and ransomware groups, making attribution of threat actors more challenging.

Economic recession, geopolitical instability and widening global inequality have increased incentives for individuals to engage in financially motivated cybercrime. Tech-savvy adolescents and young adults are especially susceptible to recruitment by criminal networks.

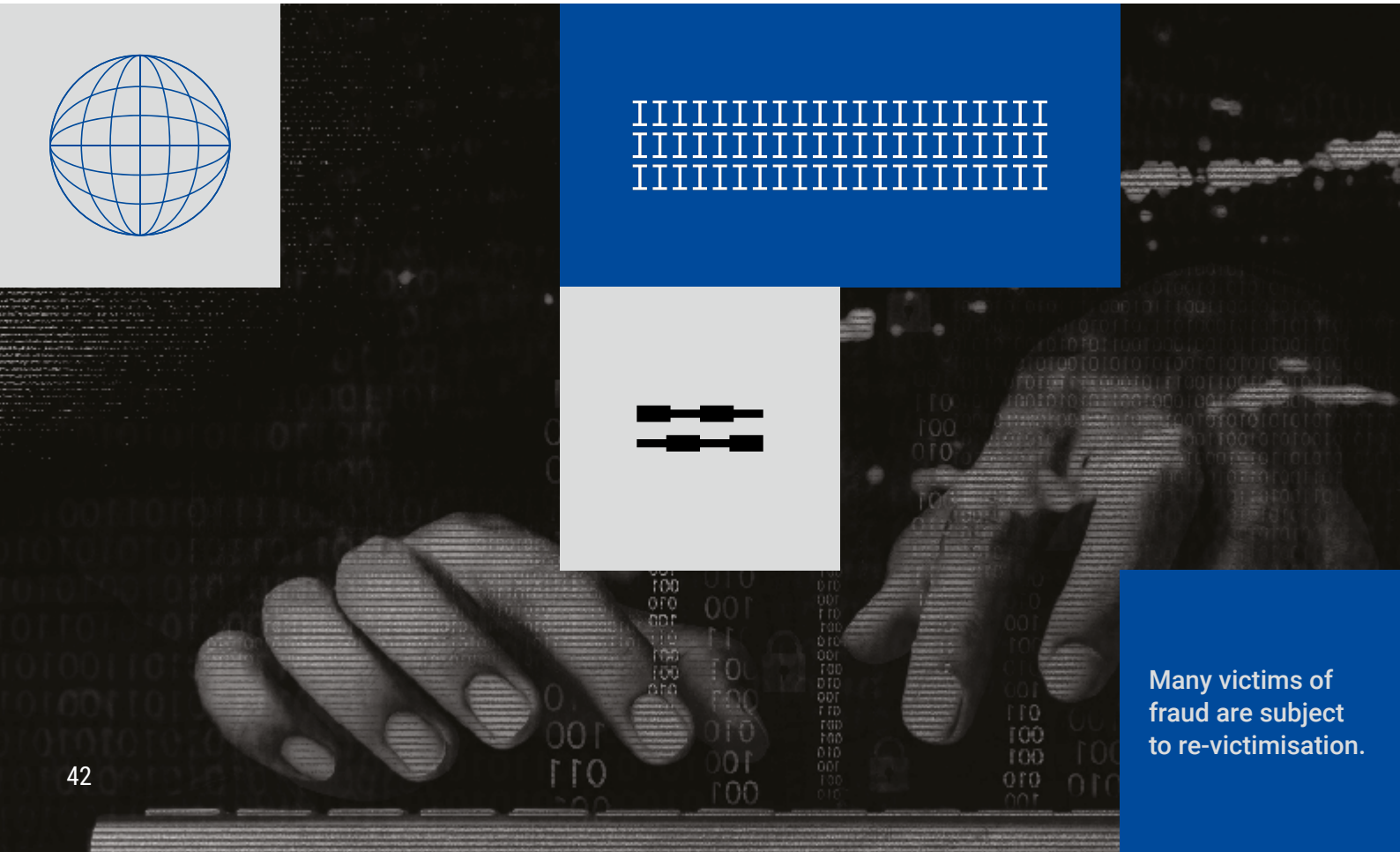


Advancements in AI will be further deployed for various aspects of cyber-attacks: for attack automation, social engineering, finding new vulnerabilities and by-passing security solutions. This will increase both the scale and efficiency of cyber-attacks.

AI and automation will further scale up the reach and volume of fraud schemes.

Online fraud schemes

Fraud schemes constitute the most rapidly expanding sector in organised crime, targeting a broad spectrum of victims, including individuals, public and private sector organisations, and their data, and generating large profits. The scale of online fraud, driven by advancements in automation and AI, has reached an unprecendented magnitude and is projected to continue growing. Narratives are extremely realistic, crafted with the help of AI, and incorporating trending societal topics. Cryptocurrency features prominently as a payment method and as an investment fraud product. The many victims of fraud suffer serious financial and psychological harm, and are often subject to re-victimisation. Investment fraud and business email compromise remain the most prolific online fraud schemes.



Many victims of fraud are subject to re-victimisation.

Investment fraud

Increasing threat driven by technology and AI

Investment fraud is one of the most common and growing types of online fraud, nurtured through the use of digital tools and accelerated by new technologies. The main types are Ponzi schemes[21], pyramid schemes[22], and advance fee frauds[23]. Cryptocurrencies remain the most significant investment fraud product in the EU. While fraudsters mostly target individuals, companies are also occasionally targeted. Criminal networks have been adapting the modus operandi to the availability of digital and AI tools and to exploit new and developing markets. The criminal threat is likely to further accelerate through the use and credibility of deepfakes, as well as the use of AI, machine learning, and automation.

CASE EXAMPLE – JuicyFields large scale Ponzi scheme[24]

In the "JuicyFields" investment fraud case, suspects lured victims into fraudulent crowdsourcing investments in the cultivation and distribution of cannabis for medicinal purposes. Upon the purchase of a cannabis plant, with a minimum investment of EUR 50, investors could collect high profits from the sale of marijuana to authorised buyers. The platform was not only present in the digital world, but upheld the image of a trustworthy legal business structure with physical offices, staff and representation at cannabis events. Initially, the 500 000 "e-growers", or digital growers, were receiving their investment returns.

In July 2022, the criminals behind the scheme abruptly removed company profiles from social media and stopped users from logging in to their accounts, thus freezing cash withdrawals. The scheme impacted a very high number of victims throughout the EU, with a total of reported damages of around EUR 645 million, but they could be significantly higher. The criminal network had a strong cross-border dimension, led by Russian masterminds, with strawmen in Germany and money laundering activities in Cyprus.

Internet-enabled investment fraud is becoming more prominent than unsolicited contacts, like cold calling. Online advertisements, including social media platforms, news sites and sponsored search engine results are the main advertisement channels used by criminal networks to attract victims.

Online frauds, including investment frauds, are often elaborate, long-lasting, and well-crafted, creating a convincing air of legitimacy. AI and automation will further accelerate this criminal activity in the coming years.

Criminal networks perpetrating investment fraud display a high level of adaptability to socio-economic trends, new markets, media, and public interest, shifting their focus to attractive emerging products.

Investment fraudsters are extremely adaptive, adjusting their narratives to socio-economic trends and shifting their focus to attractive emerging products, ranging from cryptocurrency to cannabis.

Business email compromise

Prolific online fraud schemes expected to further increase

In business email compromise (BEC) cases, fraudsters gain unauthorised access to the mailbox of an employee to intercept and analyse information contained in official correspondence. Once email accounts are taken over, spoofed or new versions are created. Fraudsters request payment, misleading victims[25] by closely resembling corporate communication style and accompanying their request with well-crafted, identical falsified documents such as invoices containing modified bank accounts[26]. Identity theft and identity fraud are an intrinsic part of the sophisticated and targeted scheme crafted around the victim.

AI, including large language models (LLMs) and deepfakes, is creating new opportunities and capabilities for criminals active in BEC. As the rapid pace of technological development continues, BEC fraud is also expected to increase. Convincing fraud emails can be easily generated with the support of LLMs, while deepfake technologies, an emerging type of impersonation replicating people's voices, images, and videos, are now being used in CEO fraud, in which fraudsters seek to trick an organisation's employees by impersonating their CEO[27].

AI, including LLMs and deepfakes, lowers the threshold for entry in the criminal market, and drives new opportunities for BEC fraud and other online frauds. This is set to continue alongside rapid technological development.

Romance fraud

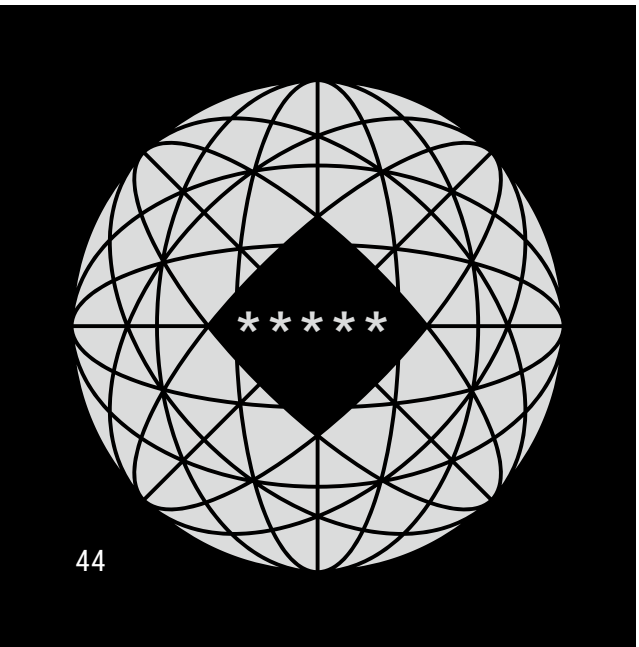
Lucrative online fraud scheme relying on profiling and social engineering techniques with enhanced realism foreseen

Criminal actors from around the globe are actively involved in romance fraud. Victims seeking companionship are approached on social media or dating sites by fraudsters, who impersonate individuals using fake accounts and profiles.

Criminals often adapt their fraudulent requests to the changing geopolitical situation, for instance, requesting money under the pretext of being victims of current conflicts or humanitarian crises. Unsuspecting victims are defrauded by being persuaded to provide financial and personal information, or to directly transfer money based on false pretexts. Targeted individuals may even be manipulated into acting as money mules. Identity theft and sexual extortion are also linked in some cases.

Romance fraud remains a lucrative online scheme, and is perpetrated mostly on dating sites, social media, and communication platforms. Criminal networks and fraudsters employ profiling and social engineering techniques to create a rapport with victims and increase profits.

Romance scams are expected to increase in the future, accelerated by AI tools. Voice cloning technology, deepfakes, LLM-generated scripts, and AI-driven translation will all continue to enhance fraudulent schemes, creating new fake scenarios and social engineering techniques.



Fraud against payment systems

High level of expertise, variation and continuous development of techniques with the future threat driven by adaptability

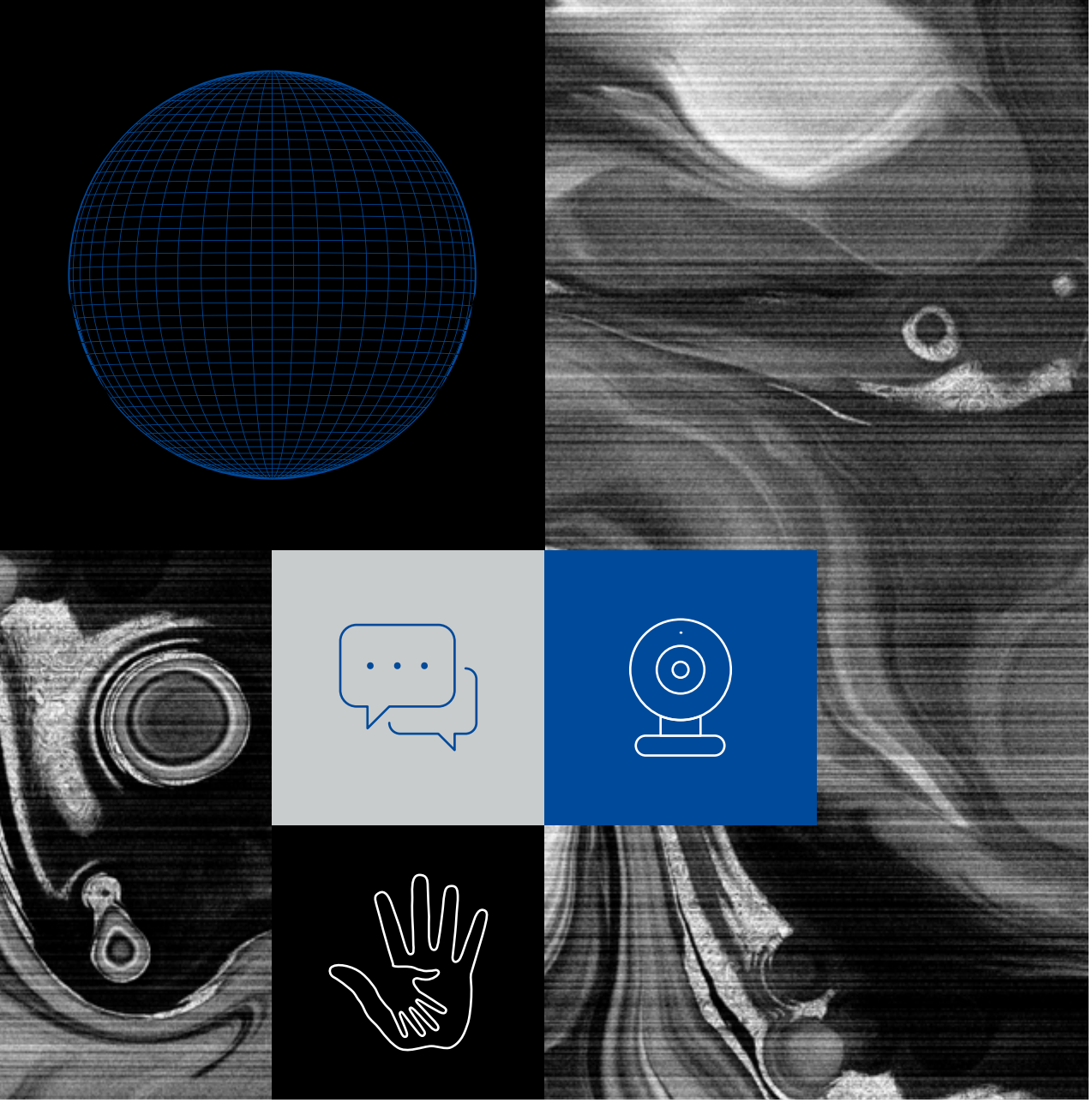
While physical skimming on bank and credit cards is rapidly diminishing in the EU, digital skimming through specific malware became more widespread[28]. Compromised card details are sold and purchased, often several times, on websites and dark web marketplaces. These are then used, for instance, in card-not-present (CNP) fraud performed by bots carrying out parallel automated purchases. There has been a major shift in digital skimming from targeting the front-end systems (such as webpages and browsers) to infecting the back-end infrastructure (server) with malware. Criminals use SIM swapping to overcome customer authentication methods.

The theft of personal data from payment systems is the main concern. Data is exploited directly or sold to other criminal actors, resulting in repeated victimisation of targets.

The fast and ongoing digitalisation of payment systems, resulting in novel payment gateways, will present new opportunities to criminal networks and require constant updates in security systems and relevant regulatory measures[29].

The modi operandi of criminal actors to defraud payment systems will continue to evolve based on further digitalisation of payment systems and fin tech developments.

Criminal actors involved in the perpetration of fraud against payment systems display high levels of expertise as it requires the development of specific malware, up-to-date knowledge of payment systems and their vulnerabilities, and the production of complex technical devices. In some cases, criminal actors who compromise payment systems also carry out cyber-attacks on other networks.



(Online) child sexual exploitation

Child sexual exploitation is a severe and impactful crime as it involves physical and psychological violence on children, heavily impacting their health and development. It is nurtured online, with online platforms providing offenders with an ever-expanding victim base to carry out sexually explicit interactions or exchange imagery within communities of offenders. It is and will be further accelerated by AI, expediting the generation of material and stepping up the scale.

Rapid evolution driven by advancements in digital technology and generative AI

Online child sexual exploitation (CSE) offences have increased in recent years, with a significant rise in the volume of child sexual abuse material (CSAM) detected online, as well as referrals and investigations. The production and distribution of CSAM is expected to grow in the future.

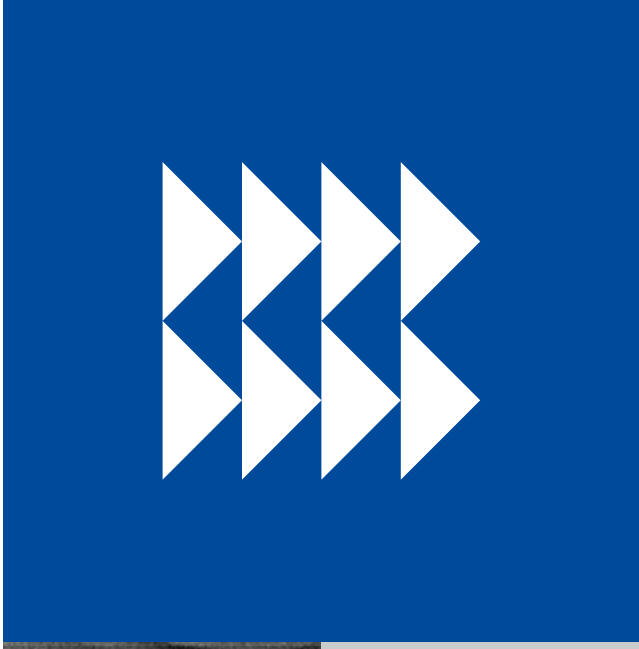
The exchange of CSAM appears to be much more frequent than in the past, likely due to the ease of use and large storage space in mobile phones, which have become the main device for the production, acquisition, and storage of CSAM. It is also increasing in severity, both in terms of the nature of the abuse and the age of victims.

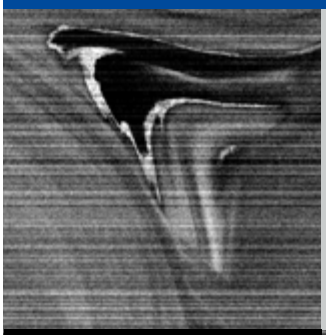
The increase in online CSE has been driven by rapid advancements in digital technologies. Most children, even very young ones, use social media and communication applications, offering ample opportunity for predators to approach their victims. The use of social media in an age characterised by self-discovery and experimentation, combined with the normalisation of online sexual behaviours (such as sexting), has contributed to the proliferation of self-generated sexual material. Sexual extortion is another ever-increasing threat.

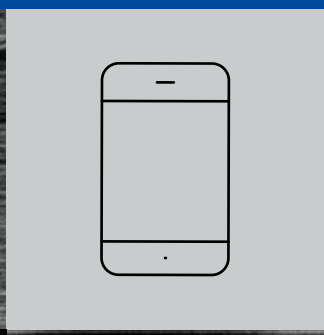
The digital acceleration has triggered a rapid evolution in online CSE. It has provided borderless platforms for offenders to create, store and exchange CSAM, and to contact and groom victims. The increased online presence of children will impact further on offenders' approaches to, and grooming and exploitation of, children.

End-to-end encrypted communication applications have created cross-border networking possibilities for offenders, both for smaller networks such as transnational child sex offenders (TCSOs)[30] and large online communities.

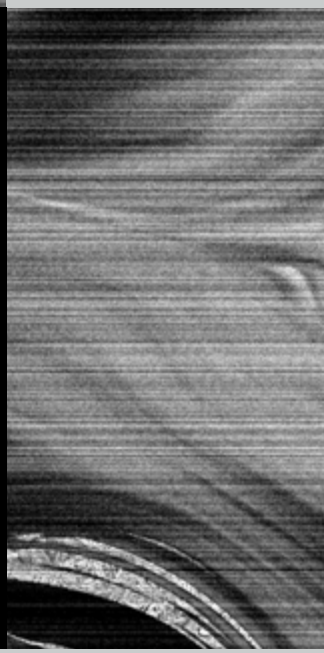
Generative AI has emerged as a new means to produce CSAM, leading to growing concerns. It can support the editing of existing CSAM and the creation of new content. Explicit pictures of adults can be manipulated to make the individual look younger or applications can 'nudify' non-explicit images. Text-to-video models have emerged, following the rapid development of text-to-image models. Given their pace of advancement, text-to-video technology is likely to evolve just as quickly[31]. In one of the first cases of its kind, a suspect was recently arrested for running an online platform with AI generated CSAM which he produced and shared around the world[32].



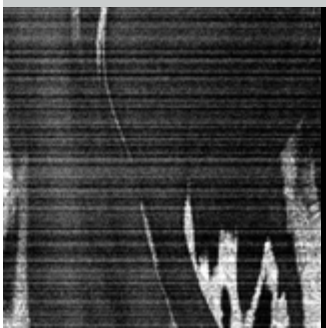




Synthetic AI-generated child sexual abuse material (CSAM) multiplies the volume of such material online.



SEVERE VIOLENCE INFLICTING SERIOUS HARM, AND RE-VICTIMISATION



CASE EXAMPLE – Symbolic monthly subscription to fully AI-generated CSAM[33]

In one of the first cases involving fully AI-generated child sexual abuse material, in February 2025, 25 arrests were made worldwide. The main suspect, a Danish national, ran an online platform where he distributed the AI-generated material he produced. Following a symbolic online payment, users from around the world were able to obtain a password to access the platform and the high-quality AI-generated CSAM. He was posting non-explicit AI-generated images of children on social media, including a link to his surface website where there would be teasers of CSAM material. The membership also gave access to exclusive communities of AI offenders. This community had around 1 500 subscribing members who were exchanging tips on how to best exploit technology to obtain CSAM and how to avoid detection.

The accessibility of AI tools has transformed the CSE landscape. Synthetic AI-generated CSAM multiplies the volume of such material online, creating additional challenges in the analysis of imagery for victims and offenders identification.

Criminal actors

Given the large spectrum of offences constituting CSE, a wide range of offenders – with diverse profiles and different motivations – are involved in this criminal activity. Hands-on abusers, producers, distributors, and consumers of CSAM are mostly motivated by their sexual interest towards children. Criminal actors involved in financial sexual extortion and professional production of CSAM for commercialisation often show no sexual interest in children and are motivated solely by financial gain.

A variety of groups leverage digital platforms to normalise acts of extreme cruelty, extort victims, share CSAM, and radicalise individuals into violent extremism.

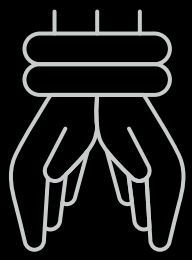
CSE offenders are becoming increasingly tech-savvy, highly aware of the security measures they can apply to protect their identities and able to rapidly adapt to changes. Most of them have the skills to develop very sophisticated countermeasures to avoid or deceive law enforcement investigations.

IT solutions for encrypted communication, streaming, file exchange as well as AI tools will enhance offenders' countermeasures and shift CSAM production methods.

The majority of offenders take part in online communities on the dark web and clear web, including forums, groups, and chatrooms. They discuss abuse, fantasies, how to acquire original CSAM, techniques to groom children and tips related to operational security. Offenders also use online means other than chatrooms for one-on-one interactions, with different levels of encryption and data transfer methods. Closed online groups on end-to-end encrypted communication applications are often international, with some having a large and long-term membership base.

Offenders who engage in direct abuse vary in profiles, ranging from middle-to-late-age perpetrators with direct access to children – either by profession or family ties – to offenders who are underage themselves. Many exhibit little to no understanding of the harm they are causing to their victims. In many cases, they describe their relationship with victims as one of love and care and do not perceive themselves as a threat to the child. Hands-on abusers are characterised by an extremely high level of recidivism.

The use of physical and psychological violence, including torture, for a prolonged duration heavily impacts the health and development of victims.



Trafficking in human beings

Trafficking in human beings (THB), for sexual or labour exploitation in particular, remains a substantial criminal market within the EU and its Member States. It is a phenomenon with global interconnections and increasingly nurtured by the online domain. It usually takes place within closed communities or environments. Criminal networks tailor modi operandi to evade law enforcement detection while increasing profits, and victims are manipulated so that they seldom consider themselves to be a victim. Yet, trafficking in human beings profoundly impacts the physical and mental health of numerous victims.

Driven into the shadows by the online domain and criminal networks' manipulation tactics

In a crime area where individuals are exploited as a commodity, criminal networks target and deceive people who are in a vulnerable position because of their security, economic or personal situation. Economic hardship and geopolitical conflict and instability drive the supply side of THB. Economic inequalities cause many victims to fall prey to traffickers' deceptive promises of better jobs and living conditions. Poverty and a lack of employment opportunities heighten this vulnerability, which is further exacerbated by geopolitical crises that may push people to seek opportunities outside their countries of origin. Combined with sustained demand for cheap labour, sexual services or other exploitative circumstances, THB is, and is expected to remain, a persistent phenomenon.

The online dimension and technological developments are central to orchestrating different forms of THB and driving them into the shadows of the criminal world. Criminal networks remotely identify and recruit their victims over the internet and social media, reach out to a wide customer base, avoid physical contact with victims and clients, and exchange their criminal earnings electronically, including using cryptocurrencies. The online space, including social media platforms, encrypted messaging services and online services, is also used for circulating pictures of travel and identity documents and the personal data of possible victims of trafficking to be inserted in a future forged/counterfeited document. Document and identity fraud remains a relevant part of the modus operandi of criminal networks involved in THB.

Criminal networks tailor their modi operandi to remain invisible and manipulate victims so that they do not consider themselves as victims.

Victims often endure forced labour, sexual exploitation, and other forms of exploitation and abuse, leading to long-term trauma. Criminal networks use psychological intimidation and manipulation to coerce victims into exploitation; the use of physical violence is less common. The so-called lover boy method – often used by young traffickers – along with debt bondage, abusing the victims' fears, and framing the exploitation as a form of assistance, are all examples of psychological manipulation. Such tactics bind victims to their traffickers and make it hard to prove the exploitation. These are often combined with the dispossession of identity documents and phones.

Trafficking in human beings is being further driven into the shadows, as traffickers increasingly use modi operandi that evade attention and that create the appearance of legitimacy. They deceive victims by encouraging them to voluntarily enter into an alleged business agreement, according to which the profits are divided between the victims and the traffickers. In this way, the criminals try to give the victims the feeling to not perceive themselves as victims of a crime. In some cases, the victims are presented with contracts that create the appearance of legitimacy for the criminals themselves and for the services the victims ultimately deliver.

The online dimension has become crucial in the organisation of the criminal process of trafficking in human beings.

Legal business structures are misused frequently for the exploitation of victims of THB. Victims of sexual exploitation are exploited in short stay accommodations, hotels, massage parlours, night clubs. Victims of labour exploitation are exploited in nail salons, shops, hospitality, construction, agriculture, etc.[34]. These businesses are sometimes owned by members of the criminal networks. Criminal networks cooperate with employment agencies and sub-contracting companies to provide a façade of legality and provide contracts and paperwork including victims' work visas and other immigration documents.

Global inequalities will continue to be a driver for criminal networks seeking to make profit. Both demand and supply of sexual services, cheap labour and other forms of THB will remain high. Ongoing conflicts in the EU's neighbourhood and beyond continue to offer favourable environments for recruiting victims. Similarly, unaccompanied minors travelling to and through the EU and its Member States will remain vulnerable to criminal exploitation in whatever form.

Criminal networks

Adaptability is a key characteristic of criminal networks involved in THB. Examples are the shift of sexual exploitation to private facilities since the pandemic and the movement of victims between various cities and countries to avoid detection and prosecution. Social media platforms, some specific for certain communities, are used to recruit victims and to coordinate the criminal business. Criminal networks are running several groups at the same time to communicate with victims, clients, and associates separately. Victims also exchange information, experiences, and the possibility to work in other countries on social media groups administered by criminal networks.

Criminal networks continue to distance themselves from the actual exploitation, managing and coordinating the criminal business, including the transfer of criminal proceeds, remotely.

Both criminal actors and victims of THB originate from within and outside the EU. There is often a link between the nationality of criminal network members and the victims.

CASE EXAMPLE – Chinese criminal network involved in THB for sexual exploitation[35]

A Chinese criminal network recruited Chinese victims using online platforms and instant messaging apps promising them a legitimate job and the possibility to rapidly earn a lot. After the recruitment, victims were trafficked to Europe using fraudulent EU identity and travel documents. In Europe, members of the criminal network advertised the sexual services of the victims online and exploited them in hotels across Europe, rotating the victims between many countries, to elude law enforcement detection and meet the growing demand for sexual services. The criminal network had various branches in several EU Member States that coordinated the exploitation of the victims on instant messaging apps. Some members were dedicated to the recruitment and trafficking of victims while others managed their actual sexual exploitation.