POLICING FUTURES

STRATALKS FUTURES NETWORK

INTERPOL GLOBAL HORIZON SCAN

November 2021

INTERPOL

INNOVATION CENTRE

07 EDITION

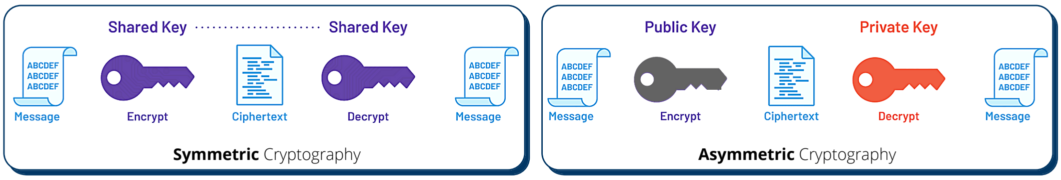
- *Trend Snapshot:* ***Criminal misuse of Cryptography***
- *Cryptography and Digitalization*
- *The challenge: criminal exploitation of cryptography*
- *New and emerging developments in cryptography*
- *Law enforcement responses to criminal misuse of cryptography: cooperation and innovation*

TREND SNAPSHOT: CRIMINAL MISUSE OF CRYPTOGRAPHY

With the advance of digitalization, cryptography has become a pervasive feature of our everyday lives, helping to protect the security and privacy of citizens and organizations alike. Unfortunately, the technology intended to keep the public safe is also being exploited by criminal networks and terrorist groups, creating significant challenges for the detection, investigation and prosecution of crime. Furthermore, the INTERPOL STRATalks Futures Network has warned that new technological developments could further complicate the situation, requiring careful monitoring. This edition of *Policing Futures* explores possible future evolutions in the **misuse of cryptography by criminal actors**. It examines the disruptive potential of technological advances like quantum computing and considers possible law enforcement responses.

CRYPTOGRAPHY IN A DIGITAL WORLD

In today's digital world, **cryptography** plays an important role in protecting individuals and organizations, helping to safeguard the **confidentiality, authenticity** and **integrity** of data. Cryptography refers to the many methods of securing information in a way that only the intended recipients can view its contents. In a computer-centric world, it is often associated with **encryption** and **decryption**. Encryption involves scrambling readable text like email or text messages, known as **plaintext**, into an unreadable form called **cipher text**. When authorized users access the protected information, it is decrypted back into its original plaintext form. The data is encrypted and decrypted through one or more **keys,** which are used with **cryptographic algorithms**, also known as **ciphers**. Generally, keys can be generated or protected by a **password**. The complexity of the cipher, as well as the ability to maintain the key a secret, determine cryptographic strength, i.e. the time and resources needed to recover the plaintext without previously knowing the key.



Symmetric and asymmetric cryptography (adapted from Qvault)

There are two main types of methods (represented above). In **conventional cryptography**, aka **secret-key** or **symmetric cryptography**, a single secret key is used for both encryption and decryption. Symmetric encryption algorithms like the widely used **AES** (Advanced Encryption Standard) are very fast, helping to encrypt anything from single files to whole disks. The main challenge of conventional cryptography is to prevent the disclosure of the secret key during transmission, known as the **Key Distribution Problem.** Addressing this issue, **public key** or **asymmetric cryptography** uses a pair of keys: a public key for

STRATALKS TREND SCAN KEY ISSUES

The STRATalks Futures Network meets regularly to identify trends, signals and other key issues affecting law enforcement. During VDRs held in September and October, STRATalks reported a number of key issues for law enforcement to continue monitoring. These include the following signals:

STRONG SIGNALS OF CHANGE

GROWING HARMFUL ONLINE BEHAVIOUR

Harmful online behavior is growing in both severity and intensity. Members of the STRATalks Futures Network warned that COVID-19 could further fuel online radicalization through its adverse effect on mental health and isolation. Other forms of harmful online behaviour, including information manipulation, cyber-bullying, harassment, and blackmailing are also on the rise. In many cases, this development is creating new duties for law enforcement. Addressing novel expectations will require raising awareness, close collaboration with private companies and academia, as well as innovative approaches.

encryption and a private one for decryption - or *vice versa* for authenticity use cases like digital signatures. Examples include the popular **RSA** (Rivest-Shamir-Adleman) and **ECC** (Elliptic-Curve Cryptography). Due to their complementarity, the two methods are often used in conjunction.

THE CHALLENGE: CRIMINAL MISUSE OF CRYPTOGRAPHY

Unfortunately, criminals around the world are increasingly misusing cryptography. **Organized crime groups, child abusers and terrorists are exploiting encrypted communications** to facilitate their illicit activities and to deny police access to evidence. When faced with encrypted data, and without the collaboration of the suspect, forensic experts can try to find the correct key or password using methods like probabilistic password guessing, memory leaks or brute force attacks. However the optimal hardware required to run such solutions is often expensive. Worse, with sufficiently strong cryptography like the widespread **AES algorithm**, it may simply be infeasible to break the encryption with existing tools. This development is particularly worrying given the broad adoption of **end-to-end encryption (E2EE)** in popular email and messaging platforms, since in E2EE systems even the service provider does not have access to the unencrypted data. According to a major forensics tool provider, on average 6 out of 10 devices reaching police labs are now locked.

Cybercriminals are also increasingly exploiting cryptography to commit cybercrimes, most notably ransomware attacks. Recently propelled to the top of security agendas due to several high profile attacks, ransomware is a form of malware designed to prevent access to files, computers or even entire servers against the will of the owner, rendering them unusable unless a ransom is paid. While there are different types of ransomware, the majority of attacks now use encryption to prevent their targets from accessing important data. Going even a step further, more and more hackers are now resorting to double-encryption to encrypt victim's data twice - and ask for two different ransoms... Beyond ransomware, **cryptography is also being abused to disguise the malware in cyberattacks.** Polymorphic viruses for instance use cryptography techniques to evade anti-virus software. In addition, according to one study nearly half of all malware in 2020 was hidden within encrypted communication channels.

As the use-cases of cryptography continue to expand, so will the risks of direct or indirect criminal misuse. For example, many **illicit activities are now exploiting the anonymity provided by the darknet**, a part of the internet where users can access unindexed web content anonymously through a variety of cryptographic and routing techniques. Similarly, some criminal groups have been known to exploit the security and privacy benefits of **crypto assets**, even if the extent of so-called crypto-crime remains contested.

NEW AND EMERGING DEVELOPMENTS IN ENCRYPTION

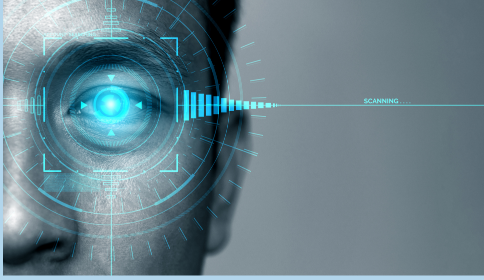
Future technological advances could bring new challenges and opportunities for law enforcement. This section discusses three important developments which police should monitor: **homomorphic encryption, quantum computing** and **quantum cryptography**. This is intended not as an exhaustive list but rather as a starting point for future exploration.

1. HOMOMORPHIC ENCRYPTION: AN OPPORTUNITY FOR LAW ENFORCEMENT?

Today, the majority of encryption systems require data to be decrypted before it can be used, creating a potential source of vulnerability. The aim of fully homomorphic encryption (FHE) is to allow data to remain encrypted even when in use. Based on different mathematical algorithms than traditional cryptography, FHE could open up new avenues for police, as there is often a need to analyze information while still protecting its privacy and security. Currently homomorphic encryption requires massive computing power, but thanks to ongoing research this barrier has been decreasing.

2. THE QUANTUM MENACE? THE DISRUPTIVE POTENTIAL OF QUANTUM COMPUTING

The development of quantum computing is often cited as the future trend with the most disruptive potential for cryptography. In theory their superior computing power could drastically reduce the time required to break popular **asymmetric** encryption algorithms like RSA. As existing quantum computers are yet to reach their full potential, analysts have noted that actors could start collecting encrypted data now and try to decrypt it once the technology matures further. Aware of these challenges, cryptographers are already researching cryptographic algorithms that would be safe to use if or when fully operational cryptographically relevant quantum computers (CRQC) emerge. For instance, the United States National Institute of Standards and Technology (NIST) is already leading efforts to standardize quantum resistant methods, which at the time of writing include several public-key encryption and key-establishment algorithms, as well digital signature algorithms. The resulting **post-quantum cryptography** could in the future emerge as a new standard, replacing existing public-key algorithms.



ONLINE FRAUD AND SCAMS ON THE RISE

Another evolving threat reported by the Network is the surge in online fraud since the start of 2021, notably romance, loan and investment scams. Enabled by digitalization, online scams are seen by criminals as a low risk, high reward activity, attracting even sophisticated organized crime operations. By some estimates, global losses to online fraud are over USD 47.8 billion. Meanwhile, prosecution rates remain relatively low, hindered by the international nature of such crimes and low reporting rates. Turning the tide on this "scamdemic" and bringing perpetrators to justice will require easier online reporting, technical solutions like Trend Micro's real-time scam detection tool, as well as enhanced global exchanges of online fraud data.

CREDIT CARD CLONING FRAUD

Several STRATalks colleagues shared that the cloning of credit cards, also known as skimming, is a growing threat in their countries. As the COVID-19 pandemic has encouraged the growth of more contactless payments, an unexpected side-effect has been the explosive growth in card fraud activity. Card cloning scams typically involve using small devices affixed to point of sales terminals (ATMs or retail locations) to steal their victims' credit card information.

WEAK SIGNALS OF CHANGE

GENDER-BASED CRIME

Many members of STRATalks have indicated that domestic violence and gender-based crimes are emerging as priority threats in their home countries, with calls for law enforcement to do more. In fact, the

3. QUANTUM KEY DISTRIBUTION

Quantum technology also holds the potential to strengthen symmetric cryptography through **quantum key distribution (QKD).** Several proof-of-concept implementations have shown that this secure method of communication using quantum mechanics could help address the aforementioned Key Distribution Problem. In practice, this technology still faces many limitations, especially over long distances, despite promising uses of satellite to ground technology.

N.B.: The INTERPOL Innovation Centre has held Virtual Training Rooms on Cryptography, Homomorphic Encryption, Quantum Computing, Crypto Assets and Darknet. To access recordings of these sessions, please contact the team at FFL@interpol.int

RESPONDING THROUGH COOPERATION AND INNOVATION

In June 2021, police in 16 countries arrested over 800 suspects who had used the encrypted messaging platform ANOM to discuss their illegal activities, unaware that the app had been secretly developed and operated by law enforcement. Known as Operation Trojan Shield, OTF Greenlight, or Operation IRONSIDE, this successful three-year-long covert investigation into transnational and serious organized crime yields three important lessons:

1. **The criminal use of encryption is a new reality which law enforcement around the world must contend with.** In its heyday, ANOM serviced over 12,000 encrypted devices, representing more than 300 criminal syndicates in more than 100 countries.
2. **Law enforcement has the potential to innovate and stay one step ahead in the encryption "crime arms race."** One of the most sophisticated operations to date in the fight against encrypted criminal activities, Operation Trojan Shield saw police successfully develop an encrypted platform and decrypt over 27 million encrypted messages over 18 months.
3. **International police cooperation is a key success factor in the fight against criminal encryption.** In the case of ANOM, synchronized action between law enforcement agencies from 16 countries resulted in over 800 arrests, the seizure of 8 tons of cocaine, 22 tons of cannabis, 2 tons of synthetic drugs, 6 tons of synthetic drugs precursors, 250 firearms, 55 luxury vehicles and over USD 48 million in various worldwide currencies and cryptocurrencies.

This and other successes prove that the global enforcement community can successfully respond to and even stay one step ahead of criminal cryptography. Carefully monitoring technological trends, adopting innovative approaches and collaborating across borders will be key.

European Parliament has called to add gender-based violence to the list of crimes to be tackled offline, online and across borders, alongside human, drug, and arms trafficking and terrorism.

ECOCIDE

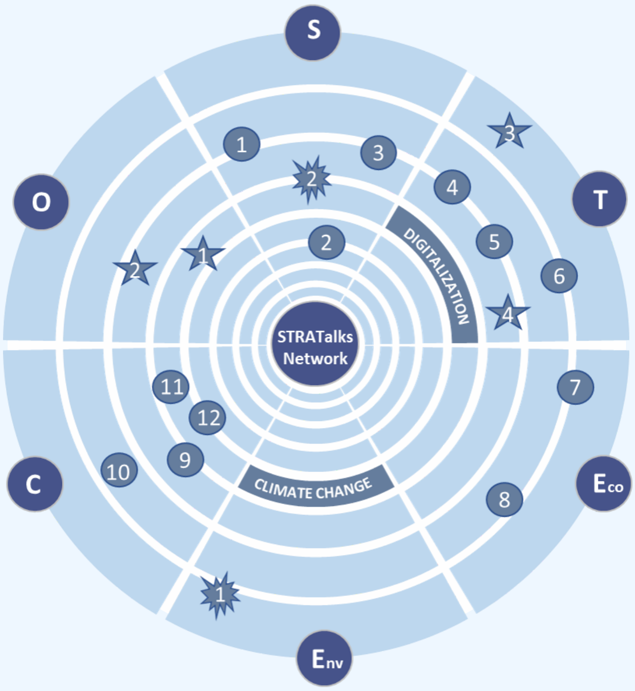
The Network also reported weak signals about ecocide, which is the criminalization of mass environmental destruction. While not yet recognized as an international crime, there is a growing movement pushing to formally establish ecocide, with the United Nations recently declaring that access to a healthy environment is a human right.

POLICING FUTURES TRENDSCASTER

The aim of the TrendsCaster is to record and visualize the trends and emerging issues identified by the STRATalks Futures Network during VDRs, using the COSTEE criterion (Crime, Organization, Society, Environment, Economy and Technology).

Strong signals

1. Social polarization
2. Growth of illegal migration
3. Online radicalization
4. Rise of synthetic media
5. More harmful online behavior
6. Digital identity
7. More cashless societies
8. Decentralized finance
9. Increasing drug trafficking
10. Violence-as-a-Service
11. Growth of online fraud
12. Ransomware



Emerging issues

- ☆1 Talent shortage
- ☆2 Future police leadership
- ☆3 Hacking the IoT
- ☆4 Criminal use of cryptography

Weak signals

- ✷1 Ecocide
- ✷2 Gender-based crime

Any additional inputs from the Network are greatly appreciated.

The STRATalks Futures Network consists of senior officials, practitioners, and strategic planners who have taken part in INTERPOL's annual strategic event. The event provides a strategic forum for discussion and acts as a global law enforcement sound board for foresight. To join the network or get in touch, please contact INTERPOL Innovation Centre at FFL@INTERPOL.INT.

2021 STRATALKS FUTURES NETWORK VDR - FUTURES SERIES SCHEDULE:

- **Session 10: 20 JANUARY 2022**