Dutch police used deep learning model to predict threats to life

Sebastian Klovig Skelton ⋮ 8-10 minutes ⋮ 5/14/2021

Dutch police developed a deep learning model in their EncroChat investigation to predict which messages contain serious threats to life

-
-

By

- Sebastian Klovig Skelton,
- Bill Goodwin, Computer Weekly

Published: 14 May 2021 10:00

The Netherlands Forensic Institute (NFI) developed software to help Dutch police filter life-threatening messages sent by suspected criminals using the encrypted EncroChat phone network.

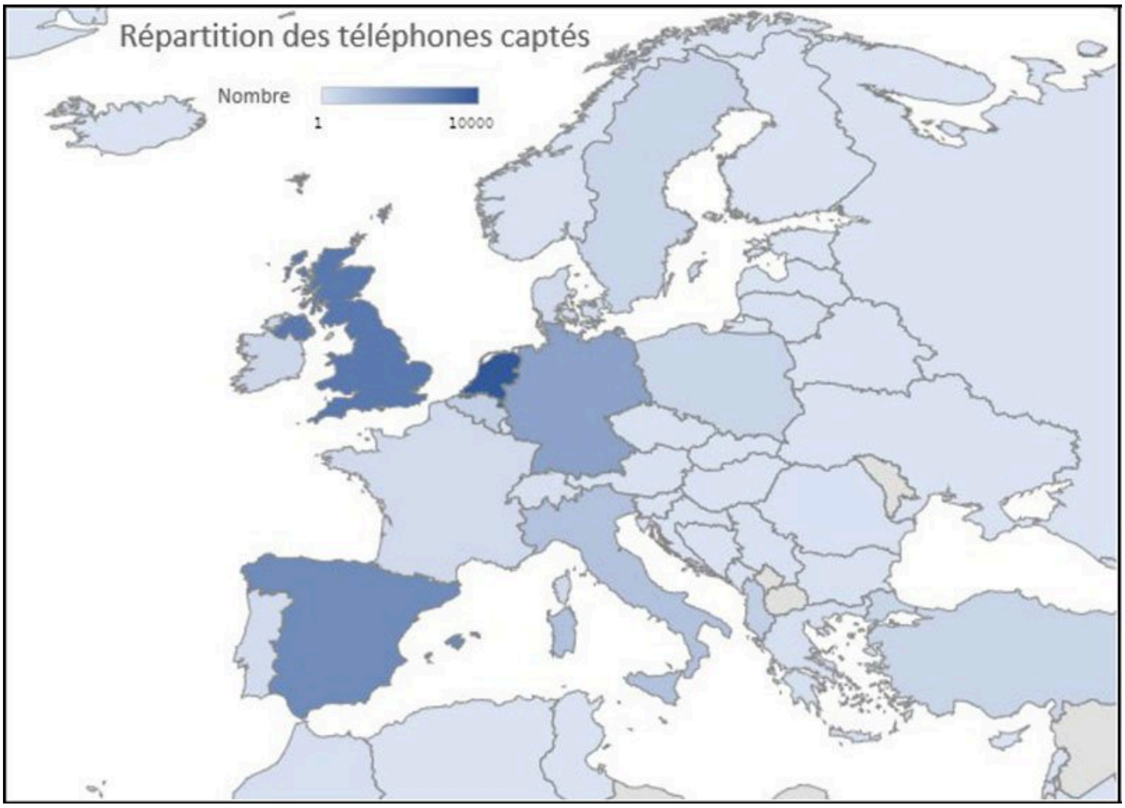
After placing a "software implant" on an EncroChat server in Roubaix, French investigators began collecting live data from phones on 1 April 2020, which they then shared with Dutch police through a secure computer link.

With the infiltration of the network leading to the interception of at least 25 million messages, Dutch police wanted a way of predicting which messages contained serious threats to life so they could take action.

To do this, the NFI's forensic big data analysis (FBDA) team modified a computer model it had previously developed in late 2019 to scan for drug-related messages sent between suspected criminals in large volumes of communications data, as part of a research and development project.

EncroChat, which had 60,000 users worldwide and around 9,000 users in the UK (*see distribution map below*), was used by organised crime groups for drug dealing, money laundering and plotting to kill rival criminals.

The NFI told Computer Weekly that the "drug-talk" software was developed in-house before being modified for "threat-to-life" detection and passed on to the police. The NFI added that the software was not used in criminal investigations during this development period.



French Gendarmarie

Global distribution of EncroChat phones

Using deep learning techniques, the FBDA team initially trained the model's neural network in generic language comprehension by having it read webpages and newspaper articles, before introducing it to the messages of suspected criminals, so it could learn how they communicate.

"The team then began using similar techniques to develop a model to recognise life-threatening messages. That model was ready when the chats from EncroChat poured into the police in Driebergen on 1 April," said the NFI in a statement.

To help the model identify which messages contained serious threats about planned murders or kidnappings, for example, the NFI created a list of "signal words" that could indicate when such crimes were about to take place.

"For example, they use the words 'dead', 'sleep', 'dolls', 'pop off', 'disappear' and so on. The police officers then labelled the results as 'threatening' or 'non-threatening'. For example, the word 'sleep' can also be used very well in a non-threatening context," said the NFI.

To prevent the model from labelling irrelevant messages as threatening, and to identify those with a high probability of being threatening, the NFI used tens of thousands of sentences containing these signal words to train it.

Because the model had already undergone language comprehension training when being taught to recognise “drug-talk”, the NFI said it only took a matter of weeks for it to learn how suspected criminals were communicating, and several more for it to distinguish whether the messages contained a threat.

While the NFI cannot guarantee 100% accuracy, the model estimates the chance of a message being threatening by scoring each on a scale of zero to one – the closer to one, the more likely it is to contain threatening content.

The NFI wrote in its statement that a human will always make the final decision to intervene when threatening messages are identified, with the model being used to highlight where they should look.

Dutch police set up a threat-to-life team and used the software to conduct automated searches for keywords that could indicate life-threatening situations.

By July 2020, Dutch investigators had warned 22 people that they were at risk of violence from criminal gangs – three months after the software spy implant went live on the EncroChat network.

Computer Weekly asked both Dutch police and the Dutch Public Prosecution Service whether either the “drug-talk” or “threat-to-life” detection software had been used in any other investigations – including the breach of the world’s largest cryptophone network, Sky ECC, by Belgian and Dutch authorities in March 2021 – but received no response by the time of publication.

Although European law enforcement authorities from a number of different countries have collaborated throughout the EncroChat investigation, a combination of the speed of the operation and different police requirements meant that each participating country built its own technology to analyse the data.

How UK authorities triaged the data

The UK’s National Crime Agency (NCA), for example, began working with the French and Dutch Joint Investigation Team and Europol to develop technology to transport and triage the EncroChat data before it was passed to the UK in January 2020.

The crime agency contributed analytical techniques and keyword searches to assist Europol in the analysis of the data.

When the implant went live on 1 April 2020, the French Gendarmerie passed intercepted messages and images to an international team at Europol based in The Hague, Netherlands.

Europol

Europol building in The Hague, Netherlands

Investigators at the Joint Operational Centre set up to analyse EncroChat data at Europol used keyword searches to identify threats to life and high-risk activity by criminal gangs, including dangers to children, the use of firearms and information relating to terrorism.

Analysts triaged to identify threats to life as the material arrived.

NCA investigators based at Europol were able to access the French Gendarmerie’s computer system to access real-time data from phones when there was an imminent threat to life.

Europol supplied British investigators with overnight downloads of data gathered from phones identified as being in the UK, through Europol’s Large File Exchange, part of its Siena secure computer network.

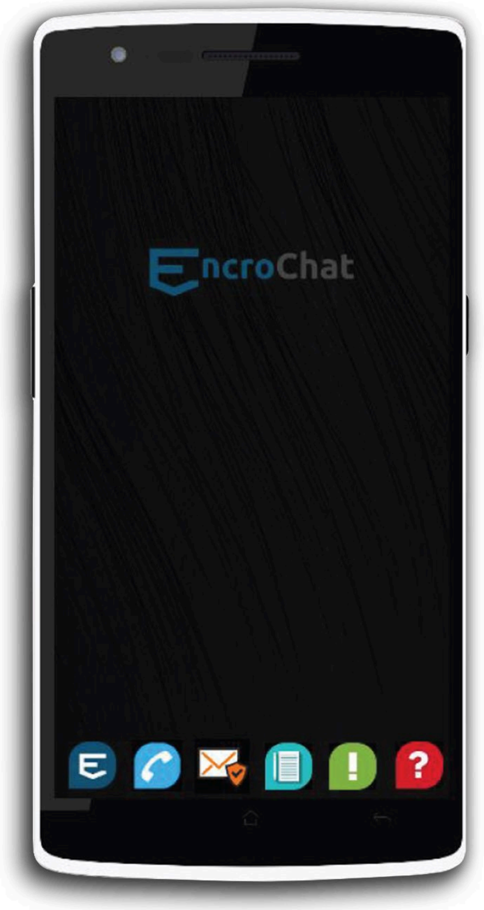
Within days, British investigators were picking up messages that showed people were in danger, as criminal gangs, whose income had fallen during the Covid lockdown, were calling in old debts.

Work began on ways to alert investigation teams to potential victims, without disclosing the source of the EncroChat intelligence, which could have alerted criminal gangs around the world that the phone network had been compromised.

Although the Dutch machine learning tool was used by the Dutch police, it was not used by other countries during the EncroChat operation.

The NCA built technology and specialist data exploitation capabilities to process EncroChat data and to locate suspected offenders by analysing millions of messages and hundreds of thousands of images.

The software, written in the Python programming language, was able to process historic messages extracted from EncroChat's in-phone database, called Realm, and live text messages sent from thousands of phones.



EncroChat phone

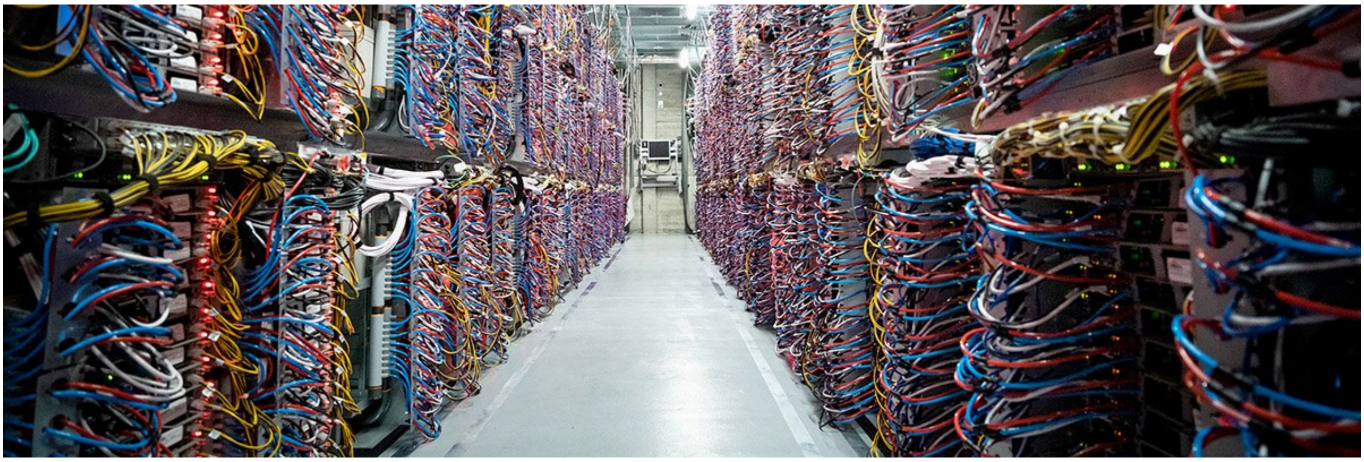
The crime agency sent intelligence packages, in the form of CSV files, to Regional Organised Crime Units, the Police Service of Northern Ireland, Police Scotland, the Metropolitan Police, Border Force, the Prison Service and HM Revenue & Customs.

They were responsible for analysing the data for further indications of threats to life, the drugs trade and other crimes.

By July 2020, working with other police forces, the NCA revealed it had prevented 200 threats to life from rival gangs carrying out kidnappings and executions.

While there is no indication that similar detection software was used in Sweden, a report published by the Swedish police's National Operations Department (NOA) said authorities had managed to avert 10 planned murders based on information from EncroChat in spring 2020.

Read more on Network software

- 

  Dutch Supreme Court approves use of EncroChat evidence

  By: Bill Goodwin

-

  Executive alleged to be behind EncroChat encrypted phone network arrested

By: Bill Goodwin

- **How the UK crime agency repurposed Amazon cloud platform to analyse EncroChat cryptophone data**

  By: Bill Goodwin

- **Forensic Institute provides Hansken viewing method for Dutch lawyers**