DELICATE BALANCE BETWEEN ANONYMITY AND LAW ENFORCEMENT

The ability to remain anonymous can be a matter of life and death for those involved in a fight for democracy. But it can also serve as a tool for criminals, who use the "darknet" for their activities. This poses challenges in police investigations.

Over the next four years, NordForsk will be providing SEK 13 million to the research project "Police Detectives on the TOR-network", a collaborative effort between the Norwegian Police University College, Stockholm University, Northumbria University Newcastle and the Open University in the Netherlands. The project will compare the everyday reality of law enforcement operations with both the forensic requirements for an investigation and the legal requirements for obtaining information properly in accordance with the statutory framework.

THE NORDIC SOCIETAL SECURITY PROGRAMME

The Nordic Societal Security Programme was launched in 2013. In connection with the programme's first call for proposals, two Nordic Centres of Excellence were granted a total of NOK 45 million:

- Nordic Centre of Excellence for Security Technologies and Societal Values (NordSTEVA)
- Nordic Centre of Excellence on Resilience and Societal Security (NORDRESS)

An international call for proposals in the area of society, integrity and cyber security was completed in March 2016 in cooperation with the Economic and Social Research Council (ESRC) and the Netherlands Organisation for Scientific Research (NWO). The following four projects were awarded a total of EUR 4.2 million in funding:

- Police Detectives on the TOR-network (A Study on Tensions Between Privacy and Crime Fighting
- Taking surveillance apart?: Accountability and Legitimacy of Internet Surveillance and Expanded Investigatory Powers
- Enablement besides Constraints: Human Security and a Cyber Multi-disciplinary Framework in the European High North (ECoHuCy)
- Governance of Health Data in Cyberspace

The Nordic Societal Security Programme is funded by the Academy of Finland, Icelandic Centre for Research – RANNÍS, Swedish Civil Contingencies Agency, Norwegian Directorate for Civil Protection, Research Council of Norway and NordForsk. The overall budget is approximately NOK 120 million.

TOR is short for "The Onion Router", an information-exchange protocol which prevents the tracking of users who send or receive data.

Normally, when you visit a website the data traffic between your device and the server computer takes the most direct route possible. While the contents of the communication may be encrypted, the IP addresses of the source and destination computers remain in readable format along the route. Otherwise the data would not reach their destination. It is possible to intercept the data traffic and see which device is communicating with which server. Web servers normally log the addresses of the computers that access them. By correlating the computer addresses with consumer data from internet service providers, the authorities can pinpoint the office or household of the person accessing the website.

Like the layers of an onion

If you use the TOR software, however, the data you send on the Internet will take a random route through some of the more than 3 000 servers on the TOR network. Each time data are relayed from one stop to another, another encryption layer is added on top of the old one, almost like the layers of an onion – thus the name "The Onion Router". The source computer will only be known by the first server, and the destination web server will log the address of the last server on the TOR network as the computer making the request, not the device where the request originated.

This makes it very difficult for authorities to find out who is posting information or accessing a website or service. No stop on the way will hold information about the source and destination of the data traffic, and even if one stop is hacked it will only be able to reveal the previous and next stop on the TOR network.

Is anonymity a good thing?

TOR originated as a research project under the US Naval Research Laboratory. Until 2012, 80 per cent of the project's annual USD 2 million budget was financed by the US Government. The Swedish International Development Cooperation Agency (SIDA) has also contributed funding, as have many organisations promoting freedom of the press and democracy.

TOR's own website stresses the positive aspects of being able to exchange information anonymously. Journalists can receive information from whistle-blowers. Volunteer organisations can allow staff members stationed in areas of conflict to communicate with their families without revealing who they are working for. Companies choose to use TOR when handling sensitive contract negotiations.

The downside is that the infrastructure can also be used for criminal purposes. Anonymity provides a cover for the distribution of child pornography, the sale of illicit drugs or activities for organising terrorist attacks.

A policing challenge

The TOR network presents a unique challenge precisely because it is difficult to unmask the flow of traffic.

The dynamic nature of TOR entails that the IP addresses used in the network change continually. Information recorded at a certain point in time will be irrelevant two weeks later. A judge or a prosecutor wishing to check a URL implicated in a specific case will find that it no longer exists. This means that investigators have to document absolutely everything by taking screenshots and recording timestamps. Otherwise, defence attorneys can claim that it was not their client who was online at a specific time.

The way in which information is compiled is also important for forensic, ethical and legal reasons.

"It is critical to maintain the integrity of the legal process throughout. This is safeguarded by following the various laws, regulations and guidelines that are in place to the letter. The retrieval of information must both be in accordance with human rights and adhere to strict scientific principles," says Professor Oliver Popov of Stockholm University's Department of Computer and Systems Sciences, who heads the research project's Swedish contingent.

"The general rule is that law enforcement agencies in one country are not allowed to gather evidence from another country without that country's consent," says Professor Wouter Stol, a former policeman who now

lectures in cybersecurity at the Open University in the Netherlands and is project leader for the overall project.

"In the Netherlands, the police work according to the general principle that as long as a server's location is uncertain the investigation may continue," he adds. "As soon as it is determined that a server is located outside the Netherlands, the police halt the investigation until such consent can be obtained. If the server is hosted in a country the Dutch police are not able to cooperate with, the entire investigation will come to a close."

International cooperation a key

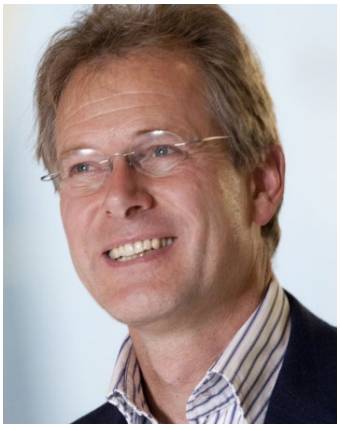
According to Professor Popov, one possibility is to try to establish a multinational platform for investigation, which could help to bridge differences in legislation between different countries.

Wouter Stol points out that international cooperation between law enforcement agencies can be effective. A recent example is from this past summer, when the Dutch police took control of Hansa Market, one of the world's largest illegal markets for drugs and weapons. For a span of one month the police took charge of administration of the site, which enabled them to collect the names of many of the site's users.

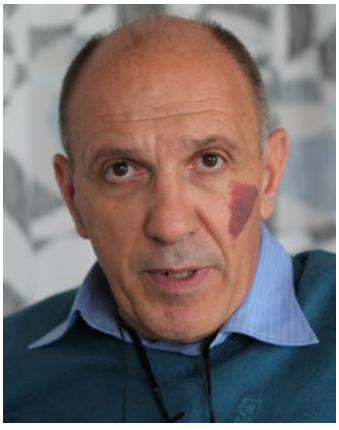
"There has been some debate as to whether the police's actions were legal or not. Is it lawful for the police to run a marketplace on the darknet? Some have accused the police of being accomplices to criminal activity, whereas others say that law enforcement needs to adopt this type strategy in the fight against crime on the darknet," says Professor Stol.

Finding the balance between the needs for anonymity and privacy on the one side with the need for effective law enforcement on the other is not going to get any easier.

"With the emergence of cloud computing and the Internet of Things, the number of sources that can generate probative evidence has increased dramatically. At the same time, artificial intelligence and data science algorithms can be of help in highly controversial areas such as predictive policing," Professor Popov says.



Professor Wouter Stol
Photo: Josje Deekens Photografie



Professor Oliver Popov
Photo: Jannecke Schulman