The Hague, 4 March 2016

EDOC # 821279v1

Considerations on the cooperation with non-law enforcement partners in the fight against cybercrime

1. Introduction

The prevention, investigation and prosecution of cybercrime calls for a close cooperation between partners from various sectors. The European Cybercrime Centre (EC3) at Europol has gained practical experience in such forms of multi-disciplinary cooperation and aims to share some of this experience through this note as input for discussions at the Conference on Jurisdictions in Cyberspace on 7-8 March 2016, organised by the Dutch Presidency of the Council of European Union.

2. The present reality

Police services at best only see the tip of the iceberg when it comes to the scale and impact of cybercrime. That is mainly due to the limited willingness of victims and witnesses of such forms of crime to report this. The expectation that such reporting will restore the losses or even get criminals convicted, is very limited, whilst the publicity around investigations and court cases is likely to have a negative impact on the reputation of the victims. This applies equally to private citizens and businesses. For companies that are not directly affected but have visibility on cybercrime, such as ISPs and Social Media, the incentives for reporting cybercrime are not always optimal either, in particular where it concerns privacy regulation and policies.

Recent initiatives have been taken to improve the reporting of cybercrime. The NIS directive is a good example. Yet the overall climate for crime reporting leaves a lot of room for further improvement.

A partial consequence of the under-reporting is that law enforcement has to ask explicitly for cybercrime related information. Both at domestic and at international level this often includes cumbersome judicial procedures, such as through MLAT. These judicial procedures are necessary to protect citizens against any arbitrary intrusion of their privacy for investigation and prosecution. An independent check of relevance, lawfulness and proportionality is needed as part of the process.

Yet, the actual investigation and prosecution is not always intended. The information may also be merely used to prevent on-going or future crimes from being committed. In those cases it is questionable whether the heavy judicial instruments are actually needed.

3. Creating a climate for enhanced cybercrime reporting

The points made in the previous paragraph invite to consider measures to stimulate a more pro-active reporting of crimes by those that suffer from them or witness them and to allow for such sharing under much easier conditions if the aim is to explicitly prevent cybercrimes from being committed.

To reach such a climate at least three elements need to be addressed: the legal basis, the need for secrecy and a change of culture.

The legal basis should provide for a couple of elements. Primarily, it should stimulate and foster the processing of data by data controllers to filter out any abuse of their services by criminals and to take action against these forms of abuse, including prevention, disruption and reporting to law enforcement. Furthermore, the legal framework should provide for the possibility to share such data under conditions of proportionality and minimisation with non-law enforcement partners with a view to help them protect themselves and their customers against forms of cybercrime. There are plenty of examples of information types that can actually be shared to prevent cybercrime at a large scale, but that are not being shared within the EU because of legal constraints. These includes fraud related bank accounts, indicators of compromise, crime related IP addresses and domain names and many more. In addition, the legal framework would ideally also enable the request of information by law enforcement for the purpose of preventing crimes through an easier and much faster procedure than the MLAT-like processes. The very nature of crime prevention calls for rapid intervention and therefore the access to information that can help to protect against cybercrime should be accommodated accordingly, yet in a structured and controllable manner. If such data would be needed at a later stage for any form of investigation and prosecution, then still the MLAT track should be followed.

In regard to secrecy, the economic consequences of crime reporting are an important reason that refrain companies from reporting crime. This can be because of reputational damage affecting the relationship with customers, but also undermine the perception of the value of the company's shares. This applies in particular if the crime is related to the theft of confidential production methods, corporate strategies or any other form of industrial espionage. For private citizens protecting the secrecy is equally important to stimulate the willingness to report crimes, especially in cases of (sexual) extortion. The secrecy should obviously apply to the entire judicial process including parts of court proceedings to the extent necessary to protect the identity and content in the interest of the victims concerned.

The third part, the climate change, requires an active debate between policy makers, companies and civil society representatives. It involves in particular the incorporation of preventive measures in the policies of among others internet service providers, telecom industry, financial services providers and social media and in their contracts with customers. These preventive measures should include warnings against abuse of their services, the data protection aspects of the service and the consequences in the event of misconduct. It is in particularly here that the balance between privacy and security can be shaped as a social contract between the general public and the Internet service industry.

4. Next steps

The considerations presented in this note are merely submitted to enrich the discussions at the afore-mentioned conference and do not constitute any official position of the organisation. In the event that questions arise in regard to the suggestions made or to the experiences with the private sector, Europol will be happy to address these.