The Hague, 13 January 2021
EDOC#1144824

Background document for the 8th Meeting of the JPSG 1-2 February 2021

Cybercrime and Digital Resilience

Technology as an opportunity for criminals to hide their tracks

For several years now, the advancement and increased implementation of certain technological developments have complicated the ability of law enforcement to gain access to and gather relevant data for criminal investigations. One of the most prominent examples in this regard remains the widespread use of encryption, which contains many benefits from a security perspective but is also a development that criminals have exploited for their advantage. Europol has spoken about this in previous iterations of the IOCTA and jointly with Eurojust in its dedicated Observatory Function reports in 2019 and 2020. In December 2020, Europol launched a decryption platform, developed in close cooperation with the European Commission's Joint Research Centre, which will significantly increase Europol's capability to decrypt information lawfully obtained in criminal investigations.

Identifying the financial trail and those facilitating it

The main motive behind the majority of cybercrime is to gain financial profit. Within EC3, one of the focal points therefore is on significantly reducing the opportunity for criminals to access their financial proceeds by dedicated actions against money mules who are part of the criminal supply chain. Between September and November 2020, participating law enforcement agencies with the support of the European Banking Federation (EBF), FinTech FinCrime Exchange, INTERPOL and Western Union, executed the European Money Mule Action (EMMA) for the sixth consecutive year. During the span of the operation, law enforcement initiated 1529 criminal investigations. With the support of the private sector including more than 500 banks and financial institutions, 4942 fraudulent money mule transactions were identified, preventing a total loss estimated at €33.5 million. As a result, 4031 money mules were identified alongside 227 money mule recruiters, and law enforcement arrested 422 individuals worldwide.

Besides actions taken to identify and arrest money mules as well as their recruiters, Operation2BaGoldMule, an unprecedented international law enforcement operation involving 16 countries, resulted in the arrest of 20 individuals suspected of belonging to the QQAAZZ criminal network which attempted to launder tens of millions of euros on behalf of the world's foremost cybercriminals

These type of operations, especially EMMA, require the ability to cooperate and exchange information with private sector partners. Access to such data for investigation purposes is crucial for any effective response against perpetrators of cybercrime as well as those facilitating the ability of criminals to hide and access their proceeds. The challenge therefore is to ensure law enforcement maintains the ability to legally access data within an environment that respects and adheres to the fundamental principles of data protection.

Identifying perpetrators and disrupting the infrastructure

Focus on disrupting criminal infrastructures and the criminals themselves is also a central feature in the approach against the Darkweb, which functions as a primary facilitator of various forms of crime. The operation DisrupTor resulted in arrests of 179 vendors of illicit goods and seizure of: $6.5 million in cash and virtual currencies; some 500 kilograms of drugs and medicine containing addictive substances; and 64 firearms. The operation shows that anonymity of Dark Web marketplaces does not provide a safe harbour for criminals. Due to effective international cooperation – in this case between Austria, Cyprus, Germany, the Netherlands, Sweden, Australia, Canada, the United Kingdom and the United States – law enforcement managed to track down the criminals.

Identifying victims and preventing re-victimisation

The detection of online child sexual abuse material continues its year-on-year upward trend, with notable exacerbation amid the COVID-19 crisis. The increased use of encrypted communication applications for one-to-one distribution of child sexual abuse material and among larger groups is also of concern. Estimates put the detection of child sexual exploitation (CSE) material in private message exchanges at up to 70%. The methods used by messaging service providers to detect child sexual abuse material do not rely on actual reading of those messages' content. Instead, they rely on matching patterns that are relevant to identifying either material or language that has been established as likely to lead to the production of that material.

With respect to child sexual abuse material, the identification of the victims is a fundamental part of the overall law enforcement response to this heinous crime. Such identification is essential to prevent further victimisation and to bring the victim to a safe place. For the eighth time, Europol held its Victim Identification Task Force (VIDTF) in November 2020, which included 23 participants from 16 agencies including INTERPOL. This first virtual VIDTF led to the identification of 9 victims and the Task Force was able to refer 53 cases to specific countries.

Robust legal bases that facilitate the work of law enforcement in the follow-up and investigation in the cyberspace arena, and support cooperation with online services providers, are thus ever more poignant. Europol welcomes the recent EU initiatives, such as the Action Plan on child sexual exploitation of July 2020, aiming at stepping up multi-sectorial response to the challenges in the combat against child sexual exploitation online. It is of the utmost importance to have a central reference point, such as a EU child protection centre, through which the efforts of law enforcement, civil society, private partners and regulators can be unified in a more effective manner. Against this background, Europol remains strongly committed in helping to pursue the EU political agenda's objectives in the fight against CSE.

Looking ahead

Besides the persistence of current threats, we are also facing the subsequent advancement and evolution of these threats. As technology continues to develop so do opportunities both for law enforcement as well as criminals. Artificial Intelligence (AI), for example, promises the world greater efficiency, automation and autonomy. At the same time, we anticipate that cybercriminals will leverage AI both as an attack vector and an attack surface. In the future, new screening technology will be needed to mitigate the risk of disinformation campaigns and extortion, as well as threats that target AI data sets. Criminals are also developing AI systems to enhance the effectiveness of malware and to disrupt anti-malware and facial recognition systems. Through enhancing and combining our knowledge about the developments, as well as their potential risks and benefits, we can work on developing a more effective response (see also White Paper on Artificial Intelligence: a European approach to excellence and trust).

Toward a more inclusive and coherent approach

Going beyond operational actions, we must look at the bigger picture with respect to how we can and need to respond to cybercrime in the longer term. In December 2020, the European Commission presented the new EU cybersecurity strategy and there are plans of introducing a Joint Cyber Unit. These initiatives are vital to ensure we are able to provide a comprehensive response to the ongoing threats faced by criminal actions. This comprehensive response needs to be inclusive and needs to acknowledge the complementary role of each stakeholder, as well as incorporate as much of the existing actions and structures to ensure avoiding duplication and overlap. Law enforcement plays a unique role in the cybercrime and security eco-system because of its core mission to identify and arrest perpetrators, disrupt criminal infrastructures as well as identify and assist victims of crime.

Involvement of law enforcement from the start of a cyber ‘incident’ is therefore essential, in order to reduce the number of victims affected and to preserve the necessary evidence to bring to justice those who are responsible for the attacks. An example of this is the EU Law Enforcement Emergency Response Protocol, in which EC3 has a central role, which serves as a tool to support EU law enforcement authorities in providing immediate response to major cross-border cyberattacks and allows for the sharing of critical information and effective cross border coordination.