Good afternoon, Ladies and Gentlemen, I am pleased to speak here to tell you about the situation concerning the fight against cybercrime in the Czech Republic.

Currently, the law enforcement and judicial authorities in the Czech Republic deal in particular with the following 4 areas of cybercrime:

1. Publicly the most visible types of cybercrime are the **ransomware attacks**. These are often targeted at hospitals and other healthcare institutions and public authorities which causes their most visible effects.

2. The second types of cybercrime which is quite strongly perceived by the public are **internet frauds** which are targeted at bank accounts, credit cards or fake e-shops.

3. The third type takes place in private and therefore its imminence is not as intensely perceived by the public as the previous types of cybercrime and it is the **child sexual abuse online.** However, it is actually very frequent and dangerous.

4. The last type is **drug crime committed online**, meaning the sale of drugs via internet. It is perceived only distantly but concerning its frequency I am convinced it is the most frequently committed online crime these days in the Czech Republic.

While the first two types of cybercrime, i.e. the ransomware attacks and internet frauds **bring profits** to the perpetrators in thousands or tens of thousands of US dollars, the second types of cybercrime, i.e. child sexual abuse online and drug crimes online make millions and even billions of US dollars. It is thus a paradox that the first two types of cybercrime are not perceived by the public as that dangerous like the other two types. It shows how we fail in the areas of providing information to public and prevention.

I can give you an example of one case the Czech Republic dealt with recently, it is called the **Sheep MarketPlace**. There was a market place located at the darknet where the trading of drugs, child pornography, weapons and other

illegal goods took place in exchange for bitcoins. After the marketplace has been revealed by the Police, it was discovered that almost 90 % of illegal trades concerned drugs, while the rest was linked to child pornography and only 3 % was the illicit arms trade. The total price of drugs trades was 18 and a half thousand bitcoins. Unfortunately, out of this number only half of one bitcoin was seized, because the perpetrator transferred the rest to normal currency. However, we managed to seize very valuable property – buildings, cars and other items in the total amount of approximately one million US dollars.

Of course the covid-19 pandemics led to the increase of all of these types of cybercrime.

Now let me finish by presenting you some of the problems we faced when dealing with these cases. When fighting cybercrime, I consider the main problem to be the tracing of perpetrators who use the anonymizing software and are thus hard to identify. Another big problem is the tracing of transfers of cryptocurrencies and encryptions of content data by the service providers.

The solution of these problems is very difficult and it is not possible to provide a simple answer. It is necessary to balance the interests of the states and law enforcement authorities on one side, and the protection of human rights and fundamental freedoms of internet users on the other side. In any case, it is absolutely clear that an efficient fight against cybercrime not only in the Czech Republic will need a much closer mutual cooperation of states and governments, as well as the cooperation of states with the private sector, for example with the service providers or cryptocurrency exchange places.

I am convinced that this is the only way which can help to clarify criminal activities in cyberspace. Therefore this approach should be taken be states as well as international organizations when considering further steps and efforts.

Thank you for your attention.