osce

УКРАЇНА 2013 UKRAINE

CONFERENCE
ON
"PREVENTION OF ILLICIT DRUG TRADE ON THE INTERNET"

Neuer Saal, Hofburg, Vienna
25-26 July 2013

CONTENTS

Executive Summary 4

H.E. Ambassador Ihor PROKOPCHUK - Chairperson of the OSCE Permanent Council 6

H.E. Ambassador Lamberto ZANNIER - OSCE Secretary General 6

Session I: The illicit drugs market on the Internet and the challenge to combat it........ 6

Mr. Adam PALMER - Senior Expert, Cybercrime, UNODC........ 6

Ms. Liesbeth VANDAM - Scientific Analyst, EMCDDA........ 7

Mr. Volodymir TIMOSHENKO - Chairman of the State Service of Ukraine on Drugs Control, Ukraine. 8

Mr. Alexey GAVRILOV- Head of Directorate, Federal Drug Control Service, Russian Federation. 9

Mr. Bilal SEN - Director of International Operations, Cyber Crimes Department TNP, Turkey. ... 10

Session II: Positive and negative lessons learned in the fight against the illicit drug trade with the use of the "shadow" Internet 12

Mr. Antii JAERVENTAUS - Expert, Pompidou Group, Council of Europe........ 12

Mr. Andrey KOMAROV- Head of International Projects, Group-IB........ 13

Detective Inspector Gerard KELLY- National Police, Irland. 14

Mr. Anton KHAZARIDI - General Directorate of Criminal Investigation, Ministry of Interior, Russian Federation........ 15

Ms. Alexandra BOBYLKOVA- Expert, Directorate of the Countering Money Laundering, Federal Financial Monitoring Service, Russian Federation. 16

Session III: Synergies among international and regional organizations, law enforcement, civil society and the private sector focused on preventing the illicit drug trade on the Internet. 17

Mr. Tony VERACHTERT -Expert, Pompidou Group, Council of Europe. 17

Ms. Beate HAMMOND – Expert, International Narcotics Control Board. 19

Mr. Vadzim VALCHOK-Senior Detective, Ministry of the Interior, Belarus. 20

Mr. Berthold BACK - Coordinator, Drugs Unit, INTERPOL. 21

Mr. Dzhurakhon ZOIROV - Head of Organized Crime Department, Ministry of Internal Affairs, Tajikistan. 22

Mr. Alexei POLISCHUCK –Ministry of Foreign Affairs, Russian Federation. 23

Closing remarks by Mr. Alexey LYZHENKOV- OSCE Co-ordinator to address Transnational Threats 24

Main findings and recommendations of the Conference........ 24

OSCE CONFERENCE
ON
"PREVENTION OF ILLICIT DRUG TRADE ON THE INTERNET"

Neuer Saal, Hofburg, Vienna
25-26 July 2013

Executive Summary

On 25-26 July 2013, supported by the Ukrainian Chairmanship, the Transnational Threats Department (TNTD) organized the OSCE-wide conference on "Prevention of Illicit Drug Trade on the Internet" in Vienna. Over 100 representatives from participating States (p.S.), Partners for Co-operation, international and regional organizations participated in this event. This year's conference was a follow-up event to the 2012 OSCE-wide Conference on "Prevention of Illicit Drug Supply to Youth". The conference on "Prevention of Illicit Drug Trade on the Internet" sustained the OSCE policy in bringing to the attention of p.S. and law enforcement agencies various tools and mechanisms of creating barriers in illicit drug trade on the Internet and of protecting young people against supply in illicit drugs. The participants shared data on new trends in illicit drugs supply and exchanged information on new methods of forensic computer investigations of drug-related crimes. They also had a unique opportunity to strengthen international and regional co-operation to combat the illicit drug trade on the Internet.

Opening remarks were made by H.E. Ambassador Ihor PROKOPCHUK, Chairperson of the OSCE Permanent Council and H.E. Ambassador Lamberto ZANNIER, OSCE Secretary General. They introduced activities of the Chairmanship and OSCE Secretariat on combating illicit drugs and encouraged the participants to constructively assess the problem of illicit drug trade on the Internet and to elaborate practical recommendations for pS and practitioners.

Session I

The illicit drugs market on the Internet and challenges to combat it

Key note speakers from, the Russian Federation, Turkey, Ukraine, the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and the United Nations Office on Drugs and Crime (UNODC) shared information on current trends in the supply of illicit drugs in the OSCE area on the Internet, including modes of website hosting, modern technologies used by criminals for illicit drug trade, encrypted communications between buyers and sellers, and means of delivery of purchased items. They raised awareness of the risks and threats posed by the online trade of illicit drugs and controlled substances and the impact on society to date. Key note speakers also introduced efforts of law enforcement agencies on operational response to prevent illicit drug supply through the Internet, measures undertaken by the participating States and assistance of the private sector in this endeavour. Furthermore, they exchanged best practices on new investigative methods for combating the illicit drugs market on the Internet.

Session II

Positive and negative lessons learned in the fight against the illicit drugs trade with the use of the "shadow" Internet

Key note speakers from the Irish National Police, the IB-Group, and the Pompidou Group, shared lessons learned, best practices and negative and positive experiences on combating the illicit drug trade on the "shadow" Internet and challenges to work with *Tor* networks. They also introduced techniques that are employed for the identification and tracing of cyber criminals; exchanged information on best practices used by law enforcement organizations and on co-operation with the private sector; called upon further interaction and co-ordination between drug control services, customs authorities, prosecutor's offices, judicial authorities as well as other competent national structures of the participating States; and promoted measures aimed at preventing trafficking in illicit drugs on the "shadow" Internet.

Session III

Synergies among international and regional organizations, law enforcement, civil society and the private sector focused on preventing the illicit drugs trade on the Internet.

Key note speakers from Belarus, Tajikistan, Pompidou Group, the International Narcotics Control Board (INCB) and INTERPOL discussed the role of relevant international, regional and national organizations in the protection of people against illicit drugs; measures to achieve synergies in their activities with relevant law enforcement agencies, consistent with their OSCE commitments and other international obligations relating to human rights, fundamental freedoms and the rule of law, and civil society to combat illicit drug supply and in particular on the Internet; and successes and challenges of international and regional assistance.

Opening Remarks

H.E. Ambassador Ihor PROKOPCHUK - Chairperson of the OSCE Permanent Council

Mr. Prokopchuk highlighted that this conference would serve as an important contribution to the implementation of the Dublin Ministerial Council Decision 4/12 on “OSCE’s Efforts to Address Transnational Threats”, including the Permanent Council Decision 1048 on the “OSCE Concept for Combating the Threat of Illicit Drugs and the Diversion of Chemical Precursors”, and would also enhance the OSCE synergies in combating the use of modern communication technologies for the illicit trade in drugs.

The speaker encouraged the conference to jointly assess the effectiveness of current legal frameworks and establish preconditions for targeted public and private sectors partnerships. He also proposed to develop awareness raising campaigns to be implemented in co-operation with the media and civil society.

H.E. Ambassador Lamberto ZANNIER - OSCE Secretary General

In his opening statement the OSCE Secretary General reviewed activities and initiatives of the organization in combating illicit drugs. He acknowledged that the Internet had been primarily designed for upright purposes, but rapidly evolving as an online marketplace for illegal goods, which included illicit drugs and illegal sales of pharmaceuticals as they contained narcotics and psychotropic substances.

He reminded participants that last year’s conference encouraged states to work together to develop new technologies to identify drug dealers on the Internet and to expand the network of computer forensic specialists to respond to this problem. He further stated that tackling this issue was a global challenge, which required mutual responsibility and effective international co-operation.

Session I: The illicit drugs market on the Internet and the challenge to combat it

Mr. Adam PALMER - Senior Expert, Cybercrime, UNODC.

Mr. Palmer underlined serious type of crimes on the Internet such as illicit drug trade, and certain illegitimate medicines (perhaps counterfeited) being trafficked in an illicit manner. He mentioned a recent study that had been conducted by UNODC on the distribution of illicit drugs. He provided three examples of websites that were being used either directly or indirectly to support the illicit of narcotics and psychotropic substances. He pointed to a website named Silk Road as an online black market, which was sometimes referred to as the deep or dark web. The latter was generally operated as a 'Tor' hidden service, so that online users could browse it anonymously and securely despite any traffic monitoring.

The "bitcoin" payment had been highly publicised recently and as a result, was now receiving a great deal of attention. It was referred to as a crypto-currency. The location and transfer of bitcoins was based on an open source cryptographic technical protocol, which was independent from any central authority. Bitcoins could be transferred through a computer or smart phone without any intermediate financial institution. Bitcoin was accepted online by trade merchants and individuals in almost every part of the world and like other currencies it could be used for illegal drug trafficking and other purposes that might constitute illegal drug trafficking or sale of illegal narcotics.

He pointed out the four core elements of UNODC's mandate related to cybercrime. These included several ways of addressing the issue; integrating it into criminal justice support; providing technical backup; training and strengthening assistance and capacity partnerships. He emphasised that the UNODC Global Cybercrime Program was designed to assist developing countries by supporting them to prevent and combat cybercrime through a global, sustainable and holistic approach. There were four activity areas: Capacity Building, Prevention, Framework Support and Co-operation. There were also two normative areas, which included providing technical assistance tools and improving standards in human rights laws.

He provided examples on distance learning training for some countries, which covered hardware concepts, operating systems, mobile forensics, smart phones, basic concepts of network and desktop forensics.

Ms. Liesbeth VANDAM - Scientific Analyst, EMCDDA.

Ms. Vandam provided an overview on the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) research on illicit drug trends in Europe.

She stated that there were around 1.4 million opiate users in Europe, which meant one in every 250 adult citizens, which was 0.4 per cent of the European population.

Cocaine as the most commonly used illicit stimulant drug in Europe with its high prevalence being mainly in Italy, Spain, the UK and Denmark. There had been an increase in the popularity of cocaine since the beginning of this millennium, although the rate of cocaine consumption had been stabilising or even decreasing, particularly in the high prevalence countries.

The other most commonly used illicit drug in Europe was cannabis. An estimate 77 million adults had used cannabis once in their life (24 per cent of the European adult population). There were major varieties within the different European countries but in general there was a stable decline of cannabis use in Europe.

The speaker discussed amphetamines and ecstasy. She identified amphetamine as the most widely produced, trafficked and used product in Europe. Amphetamines were regarded as a European drug. 1.8 million of the young adults aged between 15-30 years and 1.7 million of the European youth/adults had consumed amphetamine within the last year.

She provided details on the New Psychoactive Substances (NPS) that were identified via the early warning system. She highlighted that 73 new psychoactive substances had been reported to EMCDDA in 2012. The NPS referred to were not controlled by the international drug control instruments despite the fact that they mimicked the effect of the existing illicit drugs. Since the introduction of the early warning system, nearly 300 new psychoactive substances had been notified. In 2012, the majority of these had been synthetic cannabinoids mimicking the effect of cannabis.

She pointed out that one of the main drivers behind the increase in sales in NPS was the Internet. These new substances were marketed and distributed through the Internet. The Internet was an information hub for both the users and the producers of these drugs as the information was easy accessible on the effect of the NPS, the synthesis and the availability on the market.

Since 2006, EMCDDA had been monitoring the Internet for so called ‘online shops’ by linking the names and sizes of NPS, the marketing techniques criminals used and geographical distribution. There had been a sharp increase in the number of online shops selling so called ‘legal highs’ to EU consumers. In January 2012, almost 700 Internet shops had been in that field and this demonstrated what could be done with monitoring.

Mr. Volodymir TIMOSHENKO - Chairman of the State Service of Ukraine on Drugs Control, Ukraine.

Mr. Timoshenko highlighted the importance of this topic and expressed concern that the measures to counteract the illegal use of the Internet were not comprehensive enough. He stressed the fact that Ukraine was focused on identifying specific websites and forums that promoted drugs as well as various instant messaging, social networking and Internet-based payment sites.

He mentioned that since November 2010 new legal powers had allowed the authorities to unite various investigative forces and practice that could play a very useful role to reduce the illicit drug trade on the Internet. However, the Internet offered other means for drug dealers to make use of new opportunities: via post, DHL, TNT and other consignment companies. Controlled drug deliveries were an area Ukraine had been working in together with Russia. While part of the illegal activity took place online, the delivery was usually supplied through postal services.

This issue could only be addressed through integrated technical and legal measures that were focused on the various ‘hot spots’ concerning postal consignments. The licensing of such companies and services could have an impact on this type of crime. In some cases postal consignments did not always go through customs services and they were not necessarily being scanned.

He stated that with regard to the Internet in Ukraine it had also been established that 80 to 85 per cent of drug offers were fraudulent and there were no drugs supplies behind them. The payment occurred anonymously and the buyer was given a false location to attend and collect the drugs once the payment had been received. In many cases this was nothing more than a fraud.

Ukraine was facing a problem regarding identity and documentation in these online drug deals. Financial transfers either took place through electronic systems or were made directly to bank accounts, often to a fictitious name that made it very complicated to identify the dealer. Currently, Ukraine had been re-assessing the registration process in this area and in future it would need to improve the methods of operational investigation.

A way forward was to step up vital international co-operation as a means for a more effective targeting of the providers, whichever legislation that might fall under, whatever country, that would enable better information exchange in apprehending criminals. Today, Ukraine was looking into the issue of introducing national legislation on norms of administrative and criminal responsibility for the sale and advertisement of illicit drugs online as well as any activities promoting the use of illicit drugs. This matter was currently being reviewed but there were still challenges to resolve this issue.

Mr. Alexey GAVRILOV- Head of Directorate, Federal Drug Control Service, Russian Federation.

Mr. Gavrilov highlighted that the Internet had been actively used for the criminal activity of information theft (banking information included), fraud and pornography. Most of the consumers were aged 15 to 35 years. They made up the demographic groups which mostly used the Internet in their daily life. This had resulted in online drug trading being possible in matters of minutes to order and reach the delivery of any substance to any point in the world.

During anti-drug operations conducted in 2011, 1,900 Internet resources had been uncovered advertising narcotic, psychotropic and psychoactive substances. In 2012, over 5,000 such resources had been identified; 3,000 of which had been on Russian Internet domains. The others had been located in domains in the USA, some Asian countries and the Pacific Ocean region.

Since 2011, the Russian Federal Drug Control Service had uncovered more than 7,000 resources during its operations; 4,931 crimes related to online drug trading had been detected, which had resulted in 400 kg of drugs being seized and 1,873 individuals being brought to justice. 937 websites had been shut down based on court decisions.

Russia introduced a Single Register of Resources, which included domain names and URLs containing illegal information. Efforts to tackle these problems came from the Russian authorities adopting the Federal Law on protecting children from information that could harm their health and development, and other legislative acts. The enactment of the law had been in November 2012, which had resulted in the Federal Drug Control Service focusing on the content of the 9,000 drugs applications, 7,500 of which contained illegal information.

Russia had introduced criminal laws for the sale of drugs, psychotropic substances and their analogues online. These crimes were punishable with 5 to12 year's imprisonment, fines and confiscation of any equipment that had been used by organized drug trafficking networks.

The concern was that despite preventive and special measures been taken, this activity would lead to greater use of *darknet*, as well as new electronic payment systems. There were proxy servers based in Europe, particularly in Germany; there were other servers located in the USA. An additional point of concern was the 'bitcoin' system due to its anonymity and lack of control that national authorities had over it and that it was attracting increasing number of users.

To solve this problem was vital. Primarily there was a need to step up co-operation on the whole spectrum of issues. He underlined the importance of information exchange on Internet payments for substances that were sent by mail services.

Mr. Bilal SEN - Director of International Operations, Cyber Crimes Department TNP, Turkey.

Mr. Sen gave a brief introduction of the Internet and its impact on society to date. Criminals were undertaking their activity by using the Internet. Law enforcement officials were able to capture the communication but due to its encryption they could not read it. He made reference to a website 'sensiseeds.com' that offered for sale cannabis seeds at discount prices. It provided advice on the cultivation, culinary and harvesting techniques that were required to be employed. Additional advice is available from YouTube.

He then referred to IPhone and Android applications that were available to help individuals address their cannabis needs and addiction levels and if necessary, refer medical advice to them covertly.

A security researcher at Carnegie Mellon University had analysed the website "Silk Road" and found out that it was selling illegal drugs and other black market items worth close to $2 million every month.

Criminals were using the Internet more frequently because the costs were much cheaper and, on the other side, law enforcement around the world had not been that successful solving online crimes.

The Electronic Commerce provided several benefits. Four different E-commercial business models were presented: 1. Business to Consumer (a website such as Amazon sells to their Customer); 2. Customer to Business; 3. Priceline (that was identified as an example for business model, where the users reveal their demands and how much they can pay and the Priceline then canvasses other companies to meet the current demand alongside the price); 4. Business to Business (such as 'Alibaba').

These were all available currently on the Internet, but the Costumer to Costumer was much more dynamic as it was untraceable. Not very much was known about this area of business but should illegal online drug-sellers go down this line it might lead to major problems for law enforcement in the future. Criminals were all aware of this new technology as it was cheaper with more available protection.

He concluded by outlining his views on the way law enforcement had to tackle online drugs. A join approach with anti-narcotic and cyber-crime units would be a start. There was a possibility of closing down websites but this was very expensive. The immediate impact would be that the criminals would create a new website within hours and carry on dealing in drug sales. Law enforcement would then need another three months to detect the new site. Consideration should be given to dealing with the consumers by providing them with more information on the risk to themselves. Test-purchase operations with a focus on the financial transactions aspect could also be contemplated with the assistance of various banking and credit card institutions. More co-ordinated and efficient activities by Customs targeting shipping in and out of the country should be a tactic to focus on. The last significant factor was the Open Source Intelligence gathering techniques that were used by Internet investigators.

Session II: Positive and negative lessons learned in the fight against the illicit drug trade with the use of the "shadow" Internet

Mr. Antii JAERVENTAUS - Expert, Pompidou Group, Council of Europe.

Mr. Jaerventaus opened his presentation by stating that if anybody wanted to "get high" a number of years ago he/she had to know the right people and had to meet them in person in order to get a drug and to pay for the purchase in cash. This was no longer the case.

If a person wished to obtain drugs now, he/she needed to just run a piece of specific software on the computer to hide the tracking on the Internet. It was easy to purchase virtual money and to go shopping in one of the anonymous market places. All this could be done safely out of the reach of law enforcement and the products would be delivered to one's doorstep through the regular mail.

The major aspect of these anonymous market places/sites was that they did not only sell drugs but also offered other kind of services and products, such as: weapons, explosives, poisons, money laundering, child pornography, etc. The traditional black market was just 'a couple clicks' away.

He stated that encryption was secure enough for the criminals to communicate safely with each other. To date it had been unbreakable to law enforcement. It was important to note that all these walls had initially been designed to build a better world, not to boost criminal activities. But they had been adopted by cryptographs and they had been now used for running services like Silk Road.

According to the data available, the size of the virtual black market was at least $26 million in 2012. This market was divided and run by three key players: Silk Road, the Black Market Reloaded and Atlantis. Additionally, there were some new smaller players and national markets like the Russian Rand. In July 2013, a new market place emerged called the Deep Bay. Mr. Jaerventaus' estimate was that the current size of the black market was about $50 million.

Key indicators associated with, for example, only one site such as Silk Road. There are currently more than 12, 000 vendors with some 50-60 vendors joining in the market every month. There were 30,000 to 50,000 customers in 2012 with an annual turnover of over 15$ million. The administrators of the website collected a profit of 1.1 million.

He also advised on the bitcoin market size economy, which approximately amounted to €830 million. In July 2013 the average price for bitcoin was €66.

In concluding, Mr. Jaerventaus stated that the recent developments in web technology enabled the emergence of this new global black market. That meant that access to drugs was no longer limited to social networks or geographical location. This allowed for lowering of the threshold to buy drugs and led to mainstreaming of drug using.

Mr. Andrey KOMAROV- Head of International Projects, Group-IB.

Mr. Komarov informed about cyber criminals, who operate on Silk Road, Atlantis and such type of resources. Criminals used different measures for anonymity such as Tor and P2P. The latter was the second most popular method for organizing anonymous communications through viper channels and other different underground services such as Secrets Line and VIP 72.

Group IB worked closely with law enforcement in different countries, as well as the Interpol Digital Crimes Center and Microsoft Digital Crimes Center.

An important factor concerning legislation was that in some countries there was no official law on spam and the advertisement of illegal content. Russia was currently planning to create amendment to the criminal code.

He discussed the techniques employed for the identification and tracing of cyber criminals. He said that the idea embraced the "research of Tor exit"; it could be achieved with organizing the servers within the Tor network. This could be accomplished by having a good bandwidth, good resources and good routing facilities within EU countries. For the last year, there had been a number of joint operations with law enforcement within a number of EU countries on organizing their own exit notes where it was possible to check the network flow.

It was impossible neither to get information on the entry points of the Tor connection, nor to obtain the real IP address of the criminal. However, it was possible to intercept all the traffic on the exit of this information. Such scenario helped law enforcement to intercept criminal's credentials, some signatures of his/her machine and some other helpful details. It was quite a difficult task for engineers and in some countries they were not allowed to do it.

The next scenario was related to tracing the criminals (who were not using Tor but other anonymous software), by means of VPN tunnels and proxy servers. According to Mr. Komarov, the technology that could be helpful in such investigations was Java script (Adobe flash or Java), though it could be disabled on the user's side. However, it could help in capturing the local information from the machine of the criminal: tracking the system's time could be beneficial in identifying the criminal's nationality. For instance, the Moscow-based time meant that the computer in question was located in the Russian Federation. The second stream was the criminal's local IP address. And the third one was related to the model of the criminal's cell phone. It was a user agent. The user agent's strength could be different but by means of application of some special techniques it was possible to capture it and to use it for further investigation.

The method called "Pretty Good Privacy" (PGP) consisted in e-mailing Keys money, where for example on Silk Road the users shared PGP Keys code for the encryption between the community/network members. There were some public known tools (such as PGP Dump), which could help to extract the data from the public key.

Counter forensics was a whole new direction that cyber criminals were now employing. It had already been acknowledged that the modern cyber criminals were well educated and skilled in using special measures and techniques to protect their activities, computers and cell phones from the law enforcement reach. An example to this would be a specially created hardware (such as a "magnetic wiping") which culminated in the complete machine destruction by a simple "push of button" making it impossible for the law enforcement forensics to retrieve any data.

Currently, the encryption was a major challenge on the way to counter the cyber criminality but nevertheless, some new methods had recently been developed to decrypt PGP by seizing or obtaining their private keys. It was a very complicated process that required a compromise of the criminals' computer in an effort to obtain the special software like key loggers, or other specialised property in order to extract the key and to use it for further decryption between the community/network members.

Detective Inspector Gerard KELLY- National Police, Irland.

Mr. Kelly provided a brief background of the National Police Force of Ireland and identified a number of specialised units, which included the serious crime squad, national drug unit, fraud squad, and the criminal assets bureau.

He began his presentation by focusing on head shops, the Psychoactive Substances Act of 2010 and Test Purchasing operations which had just commenced in relation to Silk Road and trafficking on the Internet. In 2005, there had been six head shops operating in Ireland. Within four years it had nearly quadrupled. Internet drug online outlets went from 170 in 2010 to 693 in 2012.

The head shops had operated by selling cannabis seeds, cigarette wrappers and paraffin largely associated with herbal cannabis industry. It was not an offence in Ireland to sell cannabis seeds or to have possession of cannabis seeds, while the possession of a cannabis plant was a criminal offence. The head shops in Ireland were operated to make money. Over the last four years there had been an enormous increase in drug consumption due to New Psychoactive Substances (NPS) which he described as legal highs, party poppers, party-drugs. There was no legislation in Ireland to deal with these new drugs. The drugs were attractively packaged and focused at the 15 to 35 years age group and mimicked cocaine and herbal ecstasy. They were then broken into the various groups such as cathinones, synthetic cannabinoids, piperazines, phenethylamines and trypatamines.

Furthermore, criminal networks were using BZP instead of ecstasy, recently. Over the past 4 to 5 years, the seizures of ecstasy had dropped off completely in Ireland. Seizures were approximately a million tablets a year. Recent years has seen a saw small amount being seized. In the last six months, half a million had been seized. Apparently, there was problem of a shortage of precursor chemicals in laboratories in Belgium and Holland. They substituted another substance for PMK. Ecstasy consumption was increasing again.

Synthetic cannabinoids were available and had a very high content of THC (Tetrahydrocannabinol) which was four to five times more potent to the actual THC in cannabis plants.

In order to combat the head shops and the explosion of NPS, the Psychoactive Substances Act of 2010 had been introduced by the Ireland Minister of Health. This had followed the tragic death of a student who had jumped off the roof of his apartment after consuming one of those psychoactive substances. As a result, Test Purchasing Operations had commenced which had targeted the head shops, purchasing the drugs which resulted in individuals being arrested and being prosecuted. It had an immediate impact as the head shops went out of business.

Section 5 of this Psychoactive Substances Act created an offence to publish in any way or display, or advertise, or import any psychoactive substances. Section 12 empowered the police to search without a warrant any retail premises, seize and arrest in relation to any objects used for cultivation of hydroponic means. In order to prove the case in court forensic analysis needed a psycho-pharmacologist report in relation to psychoactive substance.

The police and the Irish Medicines Board monitored Irish websites on the Irish IE domain. Should any of these come to attention or were in any way involved in drugs or counterfeit medicines they were reported to the IEDR, which was the Irish Domain Registry and the website was removed.

Mr. Anton KHAZARIDI - General Directorate of Criminal Investigation, Ministry of Interior, Russian Federation.

Mr. Khazaridi's presentation outlined the successes and challenges that the Directorate for Criminal Investigation of the Russian Interior Ministry faces in countering the spread of synthetic drugs used in the Internet.

From 2010 onwards, Russian authorities have been seeing an aggressive rise in the use of synthetic drugs, primarily amphetamine type stimulants, and this was one of the reasons why it was having an impact on the rise of the Internet trade. Statistics showed that the number of Internet users in the Russian Federation reached 60% of the entire population of the country.

He stated that in 2010 – 2011 various web sites on Russian Internet appeared containing information about the sale and method of preparation of synthetic drugs, such as amphetamine, methamphetamine, methadone and synthetic cannabinoid. The monitoring of websites, chat forums and search systems allowed the authorities to uncover various sources, which included discussions on underground laboratories preparing synthetic drugs, how they could be manufactured as well as steps on how to trade. Additionally, Internet shops were discovered that specialised in selling chemicals and laboratory equipment for making amphetamines through the so-called cold method as well as other synthetic drugs. To date, the Russian authorities had shut down 30 laboratories that were producing amphetamine and methadone.

Large drug consignments were ordered on the Internet with assistance of Skype, Jubber and some other messaging programs. During communication different kinds of encoding programmes had been used to hinder the investigation.

This type of activity where criminal gangs sold drugs online using electronic payment was rather complicated and required detailed documentation of the cases and significant technical resources backup by working together with law enforcement agencies in operational co-operation to identify where the proxy servers were located.

Ms. Alexandra BOBYLKOVA- Expert, Directorate of the Countering Money Laundering, Federal Financial Monitoring Service, Russian Federation.

Ms. Bobylkova opened her presentation by describing a recent investigation on the financial flows in the Russian Federation that was linked to Afghan opiates.

She identified the connections between the Afghan drug business and the financing of terrorism. This also included the different underline factors related to crimes. Another area that was addressed related to the financial procedures required for the acquisition of precursors and substances that are vital for producing the drugs.

One of the most important techniques that she mentioned was the investigation of the suspicious nature of any financial transaction and of the associates, who carried out the monitoring and supervision within financial system. It was an attempt to identify the methodologies that allowed them to carry out the analysis of any transaction(s).

She paid special attention to the new payment systems, which include prepaid cards, mobile payments and payments made using Internet technology, specifically to payments related to drugs and for money laundering purposes. Ms. Bobylkova noted that many countries and international organizations were assisting in these investigations.

She concluded by stating that the final report would provide a future path to establish what was required to set up a system for monitoring financial transactions that would identify various connections within the drugs business that the parties were trying to ascertain; how to improve co-operation between the different bodies for monitoring and law enforcement on a national and international level. This might require re-evaluating and changing of national and international legislation. It was important to understand the mechanisms of financial flows connected to illegal trade of Afghan opiates and as a consequence to find ways to undermine the financial infrastructure of illicit drugs business.

Session III: Synergies among international and regional organizations, law enforcement, civil society and the private sector focused on preventing the illicit drug trade on the Internet.

Mr. Tony VERACHTERT -Expert, Pompidou Group, Council of Europe.

Mr. Verachtert commenced by emphasising that there was a clear need for sharing best practices and for the co-ordination of interventions against drug trade in anonymous networks. He described the Pompidou Group structure and activities. He outlined the specific activities of the Pompidou Group that had been put forward to tackle the problem of drug related cyber-crime.

He added that the easy access and anonymity might lower the threshold to buy drugs and lead to the mainstreaming of drug use. It was the unknown area at the moment with regard to figures. He was satisfied that there were methods to tackle the on-going problem as shown by some of the examples in the presentations at this conference.

He highlighted a review of some analysis that was undertaken by the Pompidou Group and was now outlined in the Pompidou Group document *Drug Related Cybercrime and Associated Use of the Internet*. He emphasised that cybercrimes were extremely innovative by nature. They created a serious challenge to law enforcement and Internet providers. There was a plan to develop a manual to address these issues but it was still in the early development phase due to the need of resources to start. However, that was not produced due to the fact that the Internet was changing rapidly.

The new developments put law enforcement authorities in a position, where they could see the criminal activity taking place on the Internet. They often had very limited resources to intercept the distribution via Internet. The orders from online sites were typically delivered through postal and or currier services, which posed a serious challenge especially to law enforcement working at airports.

There had been an increase of seizures from postal boxes and courier express shipments in certain countries. Just as drug business global prevention was taking place it also needed a global approach in mutual support and sharing of information and best practices between different actors, to which the Pompidou Group pledged to contribute. This prevented the mainstreaming of online buying of drugs. He stressed that any communication to the public about buying or selling drugs online should emphasise that it was an illegal activity.

To intervene in the "bitcoin" economy as this could be a way to attempt to identify the individuals engaged in "bitcoin" exchanges in the dedicated services and improving the monitoring of mailing and courier deliveries.

He noted that attacking the Silk Road infrastructure was a very complex task and though the Tor network was very resistant against different forms of attacks, it had already been proved that it could be infiltrated and undermined. The whole system was being built to resist attacks and taking on this approach would not seem viable without significant financial and technological resources.

The intervention point was detecting online suppliers through real world investigation despite online suppliers being able to retain their anonymity while selling drugs on the *darknet*. The procurement of the drugs had to be done in the same way as in the regular drug business. The combination of information from regular drug investigations with information received from online market places in a country of origin and other clues and possible test purchases, post marks, package fingerprints, DNA and so on might help tracking down online suppliers.

Awareness-raising as well as the identification and dissemination of the best practices could provide police officers with tools for cracking down on online suppliers.

He emphasised that decision makers were largely unaware of the newly emerging anonymous black market in the *darknet*. This was due to the lack of attention as it was still small in size however a growing trend. It was important to build international networks to ensure shared knowledge, built upon expertise, implementation of different strategies and creation of operative partnerships with service providers.

The Pompidou Group proposed to Council of Europe to create a subgroup on cybercrime and drugs. This subgroup was to serve as a platform for law enforcement officials and experts for the prevention of illicit online drug trade on the Internet. In order to engage specialists the law enforcement did not solely rely on police, customs, computer crimes specialists within police and customs but also on the private sector, notably IT companies, Internet providers etc. and on joint working activities with classical investigation and specialized IT units.

In order to develop a multidisciplinary concept or approach for control measures the Pompidou Group endeavoured to innovate and expand the knowledge base in order to create networks for building expertise, raising awareness, promoting the creation of co-ordination capacity for reporting, tracking, and analysing shipments, advocacy, exploration, development and the testing of new working models.

He concluded by saying that the required concrete working objectives were to establish a co-operation network of law enforcement and experts to develop a deeper understanding of the *darknet* drug markets, and to draw up a manual on the functioning of drug-related cybercrime to allow member states to build sustainable expertise.

Ms. Beate HAMMOND – Expert, International Narcotics Control Board.

Ms. Hammond stressed that Europe was the region with the highest Internet usage rate worldwide and it was important to discuss the problems and challenges connected to the Internet as along with the easy communication there were also several issues that needed to be urgently addressed. One of them was the sale of internationally controlled substances.

The types of websites that were selling these internationally controlled substances could be distinguished within portal sites. The sites that advertised drugs were seconded to other websites handling the sale: so-called anchor sites, where customers place their orders and pay to purchase drugs; as well as the relatively recent phenomenon of underground websites such as Silk Road or Atlantis.

A method, which had become very popular recently, was the advertising of pharmaceutical preparations through social networks such as Facebook, where one could see little adverts on a favourite page that would direct persons to sites, where pharmaceutical preparations could be purchased.

In 2010, the Association for Safe Online Pharmacies, which is composed of the pharmaceutical industry, NGOs and other associations with an interest in the safe provision of pharmaceutical preparations, discovered that 36 million US citizens had purchased medications without prescriptions at some point in their lives. Another example of this concern was hydrocodone. This drug was a very popular pharmaceutical preparation painkiller and its online pharmacy had annual sales of $ 2.9 million while its legitimate trade through regular pharmacies reached $88.000.

Other substances, which were frequently offered included ephedrine and were used to boost performance in athletes and bodybuilders. Ephedrine and its by-products were used in illicit manufacturing of amphetamine stimulant types, such as methamphetamine and were also widely available. Some of the most popular New Psychoactive Substances (NPS) included methadone. It was often used in a similar way as cocaine: put into small lines and snorted.

At the request of the CND the INCB collected data and produced analyses on all relevant information, seizures of illicit substances delivered through the mail system included. This data had now been collected for the last five years and was published every year in the INCB annual report.

In 2009, the INCB issued several guidelines to combat this danger. They accumulated the consultation process with participating governments and representatives of the pharmaceutical industry alongside with associations dealing with the Internet service providers and other companies connected to the growth of the Internet. The outcome of their work had laid the basis for the guidelines that focused on the main important areas of actions that governments should undertake, *inter alia* in area of legal and administrative actions to prevent or prohibit drug sell on the Internet.

She pointed out that meanwhile, other control mechanisms were available. A number of countries were engaged in what was called cyber patrolling: that was the monitoring of the Internet for various activities so that certain actions could be timely and duly addressed.

The issue of capacity building was constantly raised and alongside awareness being fairly low, there was often a big need for capacity building in the sense of developing and establishing what the infrastructures were and if they were capable of addressing the threat.

The cybercrime awareness had to be in line with the continuous learning process that the United Nations called for; and it should apply to all persons and authorities, who were engaged in responding to these types of threats.

Mr. Vadzim VALCHOK-Senior Detective, Ministry of the Interior, Belarus.

Mr. Valchok showed figures of January 2013 which indicated that there were more than 10,000 drug addicts and 5,000 occasional drug users surveyed by the Belarus drugs service. He added that in order to establish the true figure his presented figures should be multiplied by ten. The true figure was therefore 150,000 individuals. The drugs demand level therefore had never dropped. In Belarus the drugs trade was regulated by the Law on Drugs and Psychotropic Substances as well as Precursors, which had been in place since 2012.

The control on each individual drug was defined by the list of drugs, psychotropic substances and precursors. Its violation constituted a criminal offence. In Belarus, synthetic cannabis as well as psychoactive substances of a new kind, such as: cathinones, hencyclidineamines and trypatamines drugs had emerged in 2007. They had quickly become very popular amongst young people, who were the most advanced group of the Internet users.

Shortly after they had appeared on the market, these drugs had been added to the list of forbidden substances but there had been a short period of time when they had not been illegal. Belarus had reacted quickly to the situation by reviewing the legal practice in other countries on countering the spread of new psychotropic substances. As a result, the Ministry of Interior had introduced an amendment to the Law on Drugs and Psychotropic Substances as well as Precursors and had brought to the notion the analogues of the already existing drugs.

Belarus Police' analysis of the forum's traffic indicated that there were around 2,500 users. It was alleged that about 20 percent of them were intermediary users, while two per cent were key users. The same ratios could be traced on other Internet forums regarding the sale of illegal substances.

In conclusion, he stated that nowadays Belarus was mainly used as a transit country for drugs trafficking from the East to the West and vice versa. While amphetamines, cocaine, marijuana and hashish were trafficked from Europe and European Union countries, the heroin route ran northwards in the opposite direction from Russia to the Baltic countries and Western Europe.

Mr. Berthold BACK - Coordinator, Drugs Unit, INTERPOL.

Mr. Berthold Back outlined some activities that Interpol had commenced in 2005 and concluded in August 2012. The project had been called "Drug.net". This project had been launched as a result of the meeting with the INCB, where a request had been made to INTERPOL to create an initiative related to the Internet and drug trafficking. The project had been split into two parts: awareness raising and training aspects. A request had been made to create a global Expert Group consisting of officers that were experienced in this type of crime.

He noted that it had been quickly discovered though that this training would not be as straightforward as hoped. A three-day training programme had commenced over a three-year period from 2006 to 2008, but had faced a serious setback due to the lack of computers within certain police force. Mobile tools had been produced and furnished at the end of the training. These included CD-ROMs with certain software that would allow the officers to work either in the office, home or inside cyber cafes. USB keys were provided later that included 15 - 20 software products. This had been a practical solution.

Related to the expert group, Interpol had created a group of 15 experts from numerous countries around the world, which met two to three times a year in order to discuss current developments in this field. 280 officers from 50 countries were trained with a priority to begin in the Americas.

Training Manuals in English and Spanish had been created with the assistance of the Swedish Police. The first edition had been printed in 2006, with regular updates. The last update had been made in early 2011 and needed to be reviewed as there was no information with regard to Silk Road or other similar sites. The project had been closed in 2012.

He explained that the Interpol Pharmaceutical sub-directorate focused on pharmaceutical crime. What continued to be a concern for INTERPOL was the level of sophisticated abilities that were being used to avoid detection during the operation "Pangea". This operation was run every year in November in nearly 100 countries. As a result, web-sites were removing products or closing down for a period of time during November. Operation Pangea VI had been run in June 2013. Over 200 agencies had participated in this activity. As a result, some 22,000 websites had been monitored and more than 13,000 had been closed.

He emphasized that more focus needed to be directed by countries on *darknet* and *deepweb* as there was no real solution to the question how to deal with them at present. The challenge of handling mass data required for court proceedings was not only an issues regarding the evidence chain but also with regard to educating the judicial service as a whole when engaged in drugs trails that could focus on thousands of online deals.

Mr. Back concluded by stating that INTERPOL was supportive of any new ideas to address the current problem and that the organization was prepared to assist countries in any way that they could.

Mr. Dzhurakhon ZOIROV - Head of Organized Crime Department, Ministry of Internal Affairs, Tajikistan.

Mr. Zoirov informed that the fast development of telecommunications international threats such as terrorism, trafficking in human beings and trade in illicit made it difficult to combat these crimes alone.

Earlier in July 2013, the OSCE and the Ministry of Interior of Tajikistan had held an International Conference in Dushanbe on the subject of cybercrime and new threats and challenges posed by transnational crime, such as: terrorism, trafficking in human beings, illicit arms trade and others. There had been representatives from national law enforcement agencies, international organizations and their missions accredited to the country. The head of the Internet Provider had also been present. As a result, Tajikistan had accepted the recommendations made by the various parties.

The speaker stated that the Internet was being increasingly utilized as a means for dealers to sell illegal substances, such as psychotropic substances. To address this issue, Tajikistan focused on crime investigations and suspects tracking. While in some countries the Internet was used for selling drugs, in Tajikistan, it was primarily used to set up new transport routes for trafficking the drugs. The national Organized Crime Unit had uncovered cases, where prisoners had used the Internet to run trafficking operations from within the prison: drugs had been trafficked from Afghanistan to other CIS countries via Tajikistan.

Some drug masterminds serving 25-year prison terms were able to obtain an Internet connection, which allowed them to sell drugs on the Internet transferring their financial gains to off-shore accounts. In the cause of several operations, law enforcement had found evidence that the drug dealers had used Skype and e-mail as a means of communication to discuss the sales of acetic anhydride and other precursors from Afghanistan through Tajikistan, as well as heroin shipments.

He stated that with the Tajikistan's entrance into the World Trade Organization, the national telecommunications network had experienced a huge boost with more than 600,000 new users visited the Internet. A majority of the population used Internet cards or public access points for Internet connections. More than 1.8 million users accessed the Internet in this way, which was equivalent to more than 50 per cent of the economically active population of the country.

Tajikistan had 29 Internet providers and 150 other forms of operators. Half a million users enjoyed fixed Internet connections, e-mail and SMS services. With the development of the IT market, Tajikistan had also been exposed to high levels of drug crimes committed in the virtual space.

He concluded that bearing in mind the requirements of international law, in 2008, Tajikistan had opened a national contact point equipped with a 24/7 Internet monitoring service with a specific focus on crimes perpetrated in cyber space. Currently, Tajikistan was looking to set up a centre to tackle cybercrime based on national and international expertise and assistance.

Mr. Alexei POLISCHUCK –Ministry of Foreign Affairs, Russian Federation.

Mr. Polischuck opened his presentation by stating that countering illegal drugs and the spread of the Internet drug trade was one of Russia's crucial priorities. Russia supported the comprehensive approach to the fight against all forms of drugs, both traditional and synthetic ones. The Russian Federation believed that the central role in this fight needed to be played by the United Nations. Russia's stance was decisively against any weakening or liberalisation on drugs, including changes to the existing international regime on drugs control implicating the notion of harm reduction and attempts to legalize certain types of drugs. These days the main drug threat originated from Afghanistan. He called for an active co-operation through the Paris Pact Initiative and for the implementation of the decisions adopted by the Ministerial Paris Pact Conference which had taken place in Vienna in 2012.

Drugs were closely connected to terrorism. Terrorism was fuelled with money gained from the drug trade. That was an issue that many OSCE states had acknowledged, so the Russian Federation believed that it was important to co-operate with the Financial Action Task Force in combating the laundering of the proceeds from the trade in opium. The growing production of synthetic drugs was of particular concern, with the main influx of these substances coming to Russia from EU countries, and particularly from the Baltic States.

The Russian Federation supported the activities of regional organizations, such as the Shanghai Co-operation Organization (SCO) and the Collective Security Treaty Organization, in carrying out the annual "Kanal" operations. A new anti-drug project had recently been developed through the NATO – Russia Council, which was an additional opportunity to enhance contacts between the Russia and NATO, as well as with CSTO and the EU Pompidou Group. Russia also paid close attention to the activities of EUROPOL and the European Monitoring Centre for Drugs and Drug Addiction.

With regard to the OSCE, Mr. Polischuck mentioned that Russia supported the development of its role in international efforts against the drug threat and was actively implementing the anti-drugs concept adopted in 2012. In addition, his country reaffirmed the proposal to set up a separate unit to counter illicit drugs within the OSCE Secretariat and to restart the OSCE's project on training Afghan Anti-Drugs Police in the Domodedovo Training Centre.

The problems and challenges related to illicit drug trade in the cyber space were that the Internet represented a global commercial project, and like any business project its goal was to make profits. In this way the interests of the Internet business crossed over with the interests of traditional business and therefore Internet requires regulation.

Closing remarks by Mr. Alexey LYZHENKOV- OSCE Co-ordinator to address Transnational Threats

In his closing statement Mr. Lyzhenkov summarized the contributions made by the key note speakers and participants. He concluded by presenting the following preliminary findings and recommendations, which were amended in this final report.

Main findings and recommendations of the Conference[1]

The OSCE Conference recognized the leading role of the UN in combating illicit drugs and the diversion of chemical precursors; underlined the positive co-operation of the OSCE with UNODC; and supported the further strengthening of the existing relationship with INCB, EMCDDA, the Pompidou Group and INTERPOL for more effective assistance to countries affected by the threat of illicit drugs in the OSCE area. The Conference recommended to:

[1] This is a non-exhaustive list which does not imply consensus among the Conference participants or endorsement by OSCE participating states, or by the OSCE Secretariat.

1. Actively implement the OSCE Concept for Combating the Threat of Illicit Drugs and the Diversion of Chemical Precursors (PC. DEC/1048) to address these challenges of illicit drug trade on the Internet by providing additional efforts and seeking new and innovative approaches for tackling the threat.

2. Undertake necessary measures by the participating States to adopt national legislation in order to facilitate prompt inclusion of psychotropic substances into the control lists and to share best practices in temporarily banning psychoactive substances, which are currently not under control of national/international legislation.

3. Disrupt the flow of illicit drugs via the Internet by building new and stronger bilateral and multilateral partnerships.

4. Promote the active information exchange between law enforcement agencies on uncovered illegal payments made by drug traffickers via new communication systems as well as postal services.

5. Enhance the technical infrastructure and ensure adequate funding of law enforcement to monitor the *dark web* area and the illegal anonymized traffic used in the Internet. The resulting fused intelligence should be used to drive counterdrug detection and interdiction operations.

6. Ensure that providers of the Internet-based payment services comply with the full range of Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) measures that include the identification of a recipient and a payer, and the reporting of any suspicious transactions to the Financial Intelligence Units (FIUs).

7. Raise awareness of law enforcement agencies and FIUs on the “bitcoin” payment that was now receiving a great deal of attention by the public and could be used for illegal activities as well. Improved control of the “bitcoin” economy could significantly reduce drug supply via the Internet.

8. Encourage the law enforcement agencies of the participating States to deny the Internet drug dealers their illicit profits and access to banking systems with the assistance of various banking and credit card institutions.

9. Develop legal initiatives for bringing to justice people who assist or disseminate information about illicit drugs via the Internet and elaborate strategies to target online vendors.

10. Consider specialized Joint Investigation Teams as a good tool to assist law enforcement agencies to tackle this threat.

11. Review the possibility to establish an International Cybercrime Board in an effort to develop recommendations on combating illicit drug trade via the Internet and to stimulate a policy response to this issue.

12. Improve police recruitment methods in selecting educated officers in relevant cybercrime departments to cope with the requirements for combating illicit drug trade on the Internet.

13. Provide law enforcement personnel with specialized training on the modern modus operandi of the online illicit drug business to ensure that law enforcement agencies are aware of the importance of digital evidence to encourage the development of a digital evidence strategy.

14. Combine training with workshops on the identification and dissemination of best practices to provide police officers with tools for apprehending online suppliers.

15. Study the possibility to develop standards of professional practice for the sale and transfer of pharmaceutical services via the Internet.

16. Improve the control of mail and express courier deliveries and enforce the prevention of the mainstreaming of online illicit drug purchases. Synergies between law enforcement, the private sector, postal services, and the Internet service providers would secure the impact and sustainability of any supply reduction intervention.

17. Consider INTERPOL and the Pompidou Group publications on combating trafficking in illicit drugs on the Internet as useful tools for law enforcement agencies to tackle the problem in a more comprehensive manner.

18. Continue conducting counter-narcotic conferences, which have in this format a particular value in improving co-operation and disseminating and sharing international best practices and experiences.

19. Contribute to the EMCDDA research with new trends and substance information.

20. Strengthen national capabilities to identify and target the links between online illicit drug trafficking and other cybercrimes to provide an adequate response. The private sector and law enforcement can develop highly productive relationships to cope with this threat.