**36/1/4/1/201500330**

**NATIONAL ASSEMBLY**

**FOR WRITTEN REPLY**

**QUESTION 3778**

**DATE OF PUBLICATION IN INTERNAL QUESTION PAPER: 23 OCTOBER 2015**

**(INTERNAL QUESTION PAPER NO 42-2015)**

**3778. Mr W M Madisha (Cope) to ask the Minister of Police:**

(1) Whether the Government is co-operating with other countries in order to update its capacity and capability in respect of policing cybercrime using the latest technology; if not, why not; if so, what are the relevant details;

(2) whether, as a result of the specified international co-operation, the SA Police Service has been able to make significant progress in apprehending and prosecuting an increasing number of cyber criminals in South Africa from 1 January 2010 to 31 July 2015; if not, why not; if so, what are the relevant details?

NW4520E

**REPLY:**

1. Yes, the South African Police Service is co-operating with other countries in order to update its capacity and capabilities in Policing Cyber Crime.

During 2011 and 2012 investigating officers of the Family Violence, Child Protection and Sexual Offences Units (FCS), Division Detective Service, received training on the online sexual exploitation of children. This training was presented through KINSA (Kids Internet Safety Alliance) by the experienced law enforcement officers from Canada and Australia. The investigating officers also received soft tools with which to detect, identify and investigate computer facilitated crimes.

During 2014 investigating officers from the FCS unit also received training, which lasted for 5 weeks, presented by the Federal Bureau of Investigations (FBI) in the United States of America (USA).

Between 2012 and 2014 investigating officers within the Detective Service also received training in the Peoples Republic of China, relating to the investigation of Cyber Crime.

The Division Crime Intelligence cooperates with other law enforcement Agencies in operational requests for investigations on certain cases and also on training interventions.

The cooperation with other countries includes training programmes developed to enhance the capabilities of members of SAPS to investigate cybercrime. In this regard, the Council of Europe, through the Global Action on Cybercrime (GLACY) Project, allocated funding for three years to build capacity and skills by providing the SAPS, DOJ, SSA, NPA and Judges with training for first responders, the development of cybercrime policy and cybercrime strategy.

The GLACY Project will continue for 36 months (November 2013 – October 2015). The specific objective of this project is to enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention on cybercrime.

Furthermore, there was an international conference on assessing the threat of cybercrime that took place on 26 and 27 March 2015 in Colombo, Sri Lanka. An invitation in this regard was extended to the National Commissioner of the South African Police Service to nominate suitable representatives to attend the conference. The Division Crime Intelligence nominated three (3) senior officers who attended a training session in Sri Lanka. The conference was attended by other member countries namely Mauritius, Morocco, Philippines, Senegal, Sri-Lanka, South Africa and Tonga.

The Division also nominated members who attended the 1st responder training for law enforcement training course on 17 to 21 November 2014 held at the St George Hotel in Centurion which was also provided through the GLACY project.

Strengthening interaction and co-operation between the Directorate for Priority Crime Investigation (DPCI) and International Law Enforcement Agencies and Prosecutorial Authorities, through the use of Mutual Legal Assistance (MLA), and communications on a formal and informal basis, specifically relating to the utilization of Information Communication Technology (ICT), proved essential in identifying the unique characteristics, crime patterns and criminal entrepreneurial tendencies associated with Organised transnational cybercrime.

The Directorate for Priority Crime Investigation (DPCI), in order to address National Priority Offences pertaining to serious cybercrime and technology enabled crime, cooperated with Law Enforcement Agencies and Prosecuting Authorities of the United Kingdom, United States of America, France, Canada, Nederland’s, Ghana, thereby establishing international benchmarking standards relating to competence and best practice investigative methodologies in addressing cybercrime.

1. Yes, significant progress has been made in the apprehension and prosecution of Cyber criminals.

During 2013 SAPS conducted an undercover operation, “Operation Spade”, after information had been received from law enforcement officers of Canada. Several arrests were made and these cases are pending in court. The operation and investigation is still continuing.

During 2014 members of the SAPS together with FBI agents arrested a computer web administrator in the Eastern Cape. The suspect had been responsible for the abuse of more than one thousand children in the USA.

During 2015 and undercover operation, “Operation Cloud 9”, was registered and investigated in conjunction with law enforcement officers of Belgium and the USA (FBI). During take down operations, arrests were made in Western Cape, KwaZulu-Natal and Gauteng relating to the manufacturing, possession and distribution of child pornography. Cases against the arrested suspects are still pending in court.

On 26 November 2011 the Cybercrime Intelligence Unit, Division Crime Intelligence, assisted in tracing a suspect named Zenwa Ugo Chukukere who was wanted by the Federal Bureau of Investigation (FBI) for cybercrime cases. The SAPS members were commended for the speedy arrest of the Nigerian national wanted by the FBI for conspiracy to commit wire fraud (internet fraud) to the value of $ 20 000 000.00 (US dollars).

On 20 May 2014 a joint operation between the DPCI, Crime Intelligence, South African Tactical Response Team, Department of Home Affairs, Interpol, US Immigration and Customs Enforcement (ICE) and Homeland Security Investigations (HSI) was conducted where 12 people were arrested in South Africa and 10 were arrested in the United States and Canada for cybercrime related activities.

The suspects were part of an international cybercrime syndicate operating from South Africa and in the USA and Canada. The investigation was initiated by HSI special agents in October 2011 after US law enforcement was contacted by a Mississippi resident who fell prey to a “sweetheart scam”. The syndicate purchased shipping labels from US Postal Service, Federal Express, United Parcel Service and DHL using fraudulent credit card information and stolen identities over a number of years. Once the merchandise reached South Africa, it was advertised for sale on the internet. The Division Crime Intelligence also assisted in this operation by identifying and confirming the addresses of the suspects. Interpol was also involved in facilitating the coordination of this operation.

The Directorate for Priority Crime Investigation (DPCI), emanating from international cooperation with law enforcement agencies and prosecuting authorities, initiated a criminal investigation during 2013, relating to transnational cybercrime. The operation named Scams “R” Us focused on a South African based cybercrime criminal enterprise, involved in mass-marketing fraud by purchasing merchandise from international distributors with stolen identity information and credit card particulars obtained from international hackers, and as a direct result of mutual cooperation between Law enforcement agencies of the United States, Canada and the United Kingdom.

The DPCI was able to coordinate this operation resulting in twenty (20) individuals being simultaneously arrested in the Republic of South Africa, Canada and the United States of America. This operation continued with the DPCI further cooperating with the United Kingdom Authorities which led to the latter making a profound breakthrough by arresting a main fugitive associated with the identified criminal enterprise at Heathrow International Airport.