INDIAN POLICE FOUNDATION

Konrad Adenauer Stiftung

INDIAN POLICE FOUNDATION FORUM MEET

In collaboration with

Konrad-Adenauer-Stiftung

The Role of Criminalistics and Cyber Forensics in Tracking and Investigation of Online Crime, Terrorism and Radicalisation

11th July 2017
3:00 pm to 6:00 pm

The Indian Police Foundation, in collaboration with Konrad Adenauer Foundation of Germany (Konrad-Adenauer-Stiftung) hosted a round table discussion on "*The role of criminalistics and cyber forensics in tracking and investigation of online crime, terrorism and radicalisation*" on 11th July 2017, at the Claridges Hotel, New Delhi. The seminar was attended by a host of dignitaries and experts from government, think tanks, the industry and civil society organisations. The discussions focused on the entire gamut of cyber issues (viz. cyber security, cyber threats, cyber terrorism, and online radicalisation), while also addressing the specific challenges to the Indian Police. The session was moderated by Dr. Madan M. Oberoi IPS, Joint Commissioner of Police, Delhi.

Speakers:

1. Dr. Madan M. Oberoi, Joint Commissioner of Police, Delhi Police
2. Mr. Pankaj Madan, Deputy Head- India Office & Head- Programmes, Konrad-Adenauer-Stiftung
3. Mr. Christian Friedrich Matzdorf, Lecturer for special tasks, HWR Berlin
4. Mr. Raghu Raman, Group President Reliance Industries, Former CEO, NATGRID
5. Mr. Arun Mohan Sukumar, Head, ORF's Cyber Security and Internet Governance Initiative
6. Mr. N Ramachandran, President, Indian Police Foundation

Mr. N Ramachandran introduced the luminaries and welcomed the attendees to the discussion. He informed the audience about the previous seminar organised by the Indian Police Foundation, in collaboration with the Observer Research Foundation (ORF) and Federation of Indian Chambers of Commerce & Industry (FICCI), on '*Cyber Crime – strategic vision and an action plan for mitigation of threats from the cyber world*' and declared the discussion as a sequel to the event. He drew attention of the audience to the recent work published by Rand Corporation, 'Radicalisation in the digital Era' which looked at fifteen case studies of terrorism; each of which were planned and delivered on the internet, according to the research. Exemplifying the study, Mr. Ramachandran explained how internet is becoming a far more powerful tool in proliferating online radicalisation.

Making his preliminary observations, Dr. Madan Mohan Oberoi listed out some of the policy issues that impact upon the investigation of online crime and cases of terrorism and radicalisation and also dwelt upon the role of criminalistics, forensics and cyber forensics in investigations. He divided his session under three different themes. 1. The rationale of the terrorists to use the medium of internet 2. Challenges faced by the law enforcement agencies. 3. Rising policy issues.

Mr. Oberoi spoke at length on the use of cyber space by terrorists for radicalisation, propaganda, recruitment and training. Crypto currencies like bitcoins have now become a potential vehicle for terrorist financing. In this connection, he drew attention to the report published by the Financial Action Task Force which acknowledged the same, although, so far there is no evidence yet which validated the use of crypto currencies by terrorists.

Terrorists also use cyber space for gathering and dissemination of information for their activities. A worrisome concern bothering law enforcement agencies is the use of relatively secure and secret communication mechanisms available on the cyber space in general and the dark net in particular. Beside Dark net being used as a communication medium, it is also becoming a market place for procurement of weapons, drugs, identity documents and other illegal services; beyond the tracing capacity of law enforcers. According to some unconfirmed reports, Dr. Oberoi stated that weapons were sourced through darknet in the recent terrorist attacks in Europe.

According to Dr. Oberoi, the biggest challenge faced by the law enforcement agencies is in terms of capacity. He observed that in most cases, discussions on capacity building in the cyber domain starts and ends at cyber forensics. He added that one cannot start from the scene of crime and reach the criminal because of the inherent difficulties of attributing in cyber space; combating cybercrime has to be a more proactive approach, an intelligence led approach. There is a need to target the infrastructure, be botnets or bullet proof hosting websites or even people who are using crime as a service model in darknet. There is a need to develop intelligence in the cyber space, cyber forensics, cyber investigation and to understand the vulnerabilities presented in IOT, Dark nets and cryptocurrencies.

Most of the cybercrime investigations gets stuck at the stage of exchange of information across countries and different jurisdictions; hence international collaboration is crucial. There are also issues in terms of attribution in cyber space- cross border investigation, internet governance. The impact of technologies like encryption and anonymization on law enforcement agencies for the purpose of investigation is huge. Since most of the meaningful investigation in cyber space will be multi-jurisdictional in nature, he probed if a platform for multi-jurisdictional operations would be possible.

One of the policy issues arising out of the above context is poor delivery due to handling of what are global challenges by routine jurisdictional responses. Dr. Oberoi emphasised the need to find an alternative to MLAPs to exchange information and a means to gather scattered information across jurisdictions and stakeholders. In case of an international collaboration, three elements are prerequisites:

1. Willingness to collaborate

2. Legal framework for collaboration

3. Capacity to collaborate.

So, there is a need to develop a minimum global capacity to combat cybercrime across all jurisdictions. Further, the debate on right to privacy vs. right to life and property is a concern. Another important issue is the powers of law enforcement with regard to search, surveillance, interception, decryption and content control, which is not restrictive to law enforcement agencies.

Mr. Pankaj Madan of KAS introduced Konrad-Adenauer-Stiftung. The foundation is associated with the Christian Democratic Union of Democracy, funded by the German government. The KAS have their offices in more than 90 different countries and they operate in tandem with the German embassy. KAS started their projects in India in 1968. The most important task of the foundation is to bring the politicians and policy makers of both the countries together to provide platforms for exchange of ideas. Mr. Madan also introduced Mr. Christian Friedrich Matzdorf, an expert in Criminalistics and Forensic Sciences.

Mr. Matzdorf talked of the new challenges in forensic sciences; emphasised the need for developing new perspectives and analysis on forensics and the need to develop strategies. He gave the examples of fingerprint detection and the application of modern analytics in processing finger print data. The other major development in cyber forensics is the use of face recognition and application of other biometric devices. He said that there is a need for planning and decision-making, based on the available resources- money, human resources and technical resources – and felt that there was a need to change the old perspectives and look at the new challenges afresh. While acknowledging the impossibility of controlling the internet and the dark-net, he highlighted the difficulties associated with understanding the many networks that have consequences on law enforcement. He concluded his talk by pointing to the huge mass of data thrown at us and the need to make sense of them by checking, filtering and the application of modern tools of data analytics. It was important to adapt to the rapid new changes in the field of cyber-space and all countries to work together, he said.

Mr. Raghu Raman drew attention to the shifting paradigms in the evolution of warfare. He talked of the paradigm shifts in the process of military organisation when the domains changed from conventional land warfare to sea, to air and to outer space. Cyber-space comes as the fifth domain. He believed that we are at the cusp of yet another paradigm shift which is the 'battle of the minds'. Though there are talks of funds and tools to fight the perceived enemy, even the USA, the country that spends the most on military in the world was not successful in stopping others from sabotaging their sensitive plans. For example, the ISIS has been using platforms such as Facebook and Twitter (Which function out of the USA) to reach out and create an extensive audience. Similarly, the US Government could not prevent the largest known espionage in history, perpetrated by Snowden. According to Mr Snowden, the tools that are being used seem impractical to fight the challenges on the ground.

Mr. Raghu Raman compared the recruitment videos that ISIS puts out, how successfully they leverage western pop-culture to their advantage to attract their audience vis-à-vis the recruitment methods followed by the military and the law enforcement agencies. For example, our recruitment rules for the military and police forces are so inflexible that we still insist on physical measurements and muscular power even while recruiting cyber experts.

He said that distinct from the previous five doctrines, the part of the brain that is being used for radicalisation is subliminal, psychological and that there was need to engage with professionals such as social scientists and psychologists. He concluded by saying that the ISIS video is much more aspirational than anything the law enforcement has today. There is a need to accept the changes in the doctrine and work on that instead of using the same old methods that will not lead to any substantial results. He called for an informed and enlightened relook at our strategies.

Mr. Arun Mohan Sukumar talked of the training projects that the ORF has been doing with mid to junior level police officers. He said that their ability to understand and absorb the new issues and to tackle them in day to day law-enforcement is routinely underestimated. He talked about the assumption that online radicalisation is an urban elite problem that affects only people who have the bandwidth to use such media. However, most of the cyber weapons that is dealt with today, are being developed in the emerging economies. Hacker units of the ISIS come from the south and south-east Asian geographies. He alluded to the examples of Kashbook and UC Browser which use very limited bandwidth for sharing of content. He also talked of policing and investigation of global crimes by giving the example of a German financial institution held to ransom by hackers in West Bengal, who were apprehended by the State criminal investigative department. He stated that law-enforcement agencies have to collaborate as the back-end data of many countries are stored in emerging economies like India. He also explored the role of private companies in the creation of counter narratives in our country.

He discussed the implications of end-to-end encryptions and whether the law-enforcement needed content or subscriber data for investigation and prosecution. From the ORF's projects with the police officers, it was observed that they build the case around the electronic evidence. So, the case is made or unmade based on their ability to extract data. He said that perhaps if one is able to create the cyber-crime scene, which may or may not involve electronic content, created through the collection of meta data and other circumstantial evidence, then it would be possible to put forward a convincing case before the court of law. He reiterated that the cyber-security problems faced by Indian law enforcement agencies are almost entirely human driven. In most of the cases that they encountered, the young police officers are extremely capable and aware of the technological services that they need, to hack, to monitor etc. But they are not able to build a case with the data they collect. In many cases the inclination of the law-enforcement officials is to use electronic information for intelligence purposes, which cannot be presented before a court of law as evidence, as a result of which the prosecution suffers. He pondered on the need of a change in mind-set for law enforcement officials, who are fairly well-equipped with technology and well-informed of technological developments, to move their goal-posts a little and to see what they can use from the electronic space to strengthen their offline case in court.