I am indeed happy to participate in the inauguration of the International Cyber Security and Policing Conference (c0c0on) of the Kerala Police here in Kochi. My greetings to all the participants.

I am happy to know that this conference started in 2008, as an initiative of Kerala Police along with Information Security Research Organization (ISRA), has grown to be an international event which is helping cyber policing and find strategies to prevent cyber crimes. With an increase of cyber crime by 60% over the last year, such platforms are indeed the need of the day. When I am with you I would like to share through this lecture a few thoughts on *Winning the Cyberwar*.

**Improbables and its Characteristics-Part-1**

Friends, when I see you all and also the composition of the personalities who hold great responsibilities, I thought of sharing one incident. The incident goes like this; an important event was to
take place the next day. Multiple agencies were in action. The next two nights were dark nights with no moon light. The other side the world was sleeping. At the Chandipur flight test range a series of 12 Trishuls were launched. Almost every two hours one launch. At the Island range at Stealth launch pad, a simulated Agni launch preparations were going on in high intensity. In Pokaran ranges, away from the action point number of rockets – PINAKA type, were put into action. At mid-day and evening, Air Force was bombarding with runway destruction bombs on the experimental runway. These are all intensified events for a particular purpose. There is a strategy of seeing beyond the event going to taking place and also aware the reconnaissance satellites of other countries were locking on purposely generated events. This was a well-planned measure of diverting the attention of snoopers. India woke up the next day with the news that three nuclear tests had been conducted on the same day and another two the next day. Friends, these events happened in India. It is an unexpected, unscheduled event in the eyes of the world. No one knew about it except three souls and their classified team. And India became a nuclear weapon state (1998). The whole event I described can be classified as more than a Black Swan, with the improbability of highest order to be expected from India and its nature.

The message I would like to convey, even though our actions are patriotic actions to make the nation strong, there are nations and their terrorist institutions definitely would use Black Swans against other nations, particularly against India. India’s
intelligence and technology level have to be of highest standards to meet such improbabilities. That means India has to invest in the generation of knowledge and ability to convert the improbable and to make Black Swan as White Swan. Technological challenges need technological solutions in the highest order of accuracy and response time.

Stand alone computers of innocent citizens

Friends, “we are witness to how e-Governance has brought in a metamorphosis in the way Government services the public. The transparency, efficiency and the speed with which business is transacted across sectors, no doubt increases productivity, brings in all-round development and important of all gives power to the Citizens. But it must be borne in mind that such conveniences bring with it several issues of security both at personal, corporate and National levels. This recognition is yet to percolate amongst us. It is often thought by everyone of us that since I am a law-abiding citizen and do not use my computer to transact business online with fraudulent intentions, there is no possibility of my computer being used without my authorisation to commit any crime either big or small or either locally or internationally. This premise of ours becomes totally wrong in cyber space if we do not strictly observe basic cyber hygiene. Instances have come to light where individual standalone computers of innocent citizens were used by criminals and non-state actors to commit major financial crimes and even to hack into sensitive systems compromising National security. Nature,
Speed, magnitude, difficulty in identification of perpetrators and with no borders & boundaries for committing of crimes compound the problem. Welcome to the strange world of Crimes in cyberspace that particularly represents a unique challenge in our history. A Challenge that is highly asymmetrical and unconventional. Hence response should be equally unconventional and swift.”

**Technology as a great unifier and performance enhancer in every field**

Here, I would like to discuss two aspects. One is Cyber terrorism and counter measures. Another point is Cyber war. The world has changed dramatically since the Cold War era and the advent of the cyber era.

Cyber is the fifth dimension after land, water, air, and outer space. Unlike the other four, no one can see or feel this Cyberspace but it is as real as the other four. In earlier years, the enemy was clear and it was fairly straightforward to identify the intelligence collection targets. Today, we are faced with a new world in which change occurs very rapidly, and the enemy is asymmetric and poses a very different challenge; the most significant threat today is foreign terrorists and terrorist networks whose identities and whereabouts we do not always know. In today’s world, Information Technology (IT) plays a crucial role in overcoming this challenge. Some of the core IT areas we consider crucial for counterterrorism, namely:

- collaboration, analysis and decision support tools;
• foreign language tools;
• pattern analysis tools;
• Predictive (or anticipatory) modeling tools.

The core information technologies are mapped as a thrust area for typical intelligence analysis process.

**Cyber Crimes and Cyber War**

Velocity, Ubiquity, Un-traceability and Anonymity of Attacks are hallmarks of cyber crimes and is one reason conventional crime has had its thunder stolen. Such a situation poses severe constraint on resources meant to respond to such attacks. Most importantly the speed and nature of response particularly from the Government have to drastically change to cope with this unique situation. Foremost change is the recognition that multiple agencies from both Government and Private sectors have to jointly work as partners to configure a response just like the way the attacks are an outcome of a coordinated and cooperative response from perpetrators of crime.

Cyber War can be fought by anyone; even an individual using his hacking skills against huge corporations, nations or even different civilizations. One single person’s malicious software can wreak havoc on computers and spread across nations and continents. The modern world’s industry, economy, institutions and even other facets of life is supported by computers and associated software. The individual could be acting alone; he could be part of a
group pursuing its inimical agenda or could be state supported, working to further the plans of the state.

Amongst various types of warfare, cyber war is the low cost option. At its simplest, all, it requires is one bright individual on one computer to originate cyber-attacks. Unlike in conventional war, where the attacker generally suffers heavy casualties, in Cyber War there is no casualty to the attacker. In this war, it is not the physical might of a soldier, the quality and quantity of equipment, the integration and orchestration of systems, or the strategic genius of a General which is tested. Eugene Kaspersky, one of the world’s best known cyber-security experts and the co-founder of the anti-virus company Kaspersky Labs, views India as being under constant attack from many different sources. He says- “I believe that massive attacks on the Indian government and corporations happen all the time, and that they are mostly successful. There is no one particular enemy, but dozens of different sources of attacks. It could be secret services of other countries, competitors of Indian companies, hacker groups who sell stolen data, and hacktivist groups interested in the public disclosure of information.” I am sure this statement has to be made inconsequential by our mission on preparations on cyber war.

**Future scenario of an organized cyber attack**

Friends, we live in a world where fundamentalist and divisionary forces are in plenty. The latest incidents in Iraq and the shooting down of the Malaysian airliner MH17 are showing that
these forces not only have numbers but also highly sophisticated technology. The day is not far when such organizations will begin cyber crimes and organise cyber terrorism from distant lands. Let me present to you the scenario of such a potential cyber war.

a. Telecom is perhaps the most vulnerable area to disrupt in the event of a cyber terrorism, causing wide spread panic and confusion. Most of the devices used by modern day telecom companies are from similar manufacturers and from 1-2 countries only, hence replicability of a cyber attack is very high through simulation process.

b. Another very critical target of the cyber attack would be the SCADA systems (supervisory control and data acquisition) used in Power Generation and Distribution. This can potentially affect railways, airlines and major critical functions needed. Delhi and Mumbai airports alone are handling close to 1500 flights a day and any major disruptions in the power system will send the ATC in collapse mode

c. Financial systems, though highly protected, have shown signs of being vulnerable to highly organized cyber crimes. Left in confusion, banks would choose to go offline from the internet leading non functioning ATMs and financial institutions and transactions would freeze, leading to confusion and rumors of collapse of trust in financial systems
d. Healthcare facilities may also get affected as any cyber attack may harm the critical data about patients, medicines and supplies. Coupled with power failure this may severely hamper the working of hospitals

e. GPS system are satellite operated and hence also vulnerable to cyber attacks – this can lead to loss of navigation on aircrafts, ships and military equipment rending them paralyzed, at least for a few minutes before recovery happens.

**Solution for countering cyber security threat**

I have two suggestions for countering the cyber security threat. One is technology upgrade in cyber security and second is investment and education in Cyber security.

**Technology Upgrade in Cyber Security**

- An empowered coordinating agency and government policy are critical to success. “A single national agency is required, which must receive information about all attacks. We cannot fight these attacks alone – information sharing is critical.”
- Intelligence agencies must continuously upgrade their technical capabilities - be it signal intelligence, communications intelligence & interception capability, monitoring, information sharing mechanisms and creation of databases of security.
• It is essential to wrap the operating systems and network layers with traditional encryption systems which will empower, protect and make our cyber assets non-vulnerable to external cyber attacks and should become a survivable system and network.

• There is a need to call in professionals - scientists, computer software and hardware experts - to impart latest skills in computer hacking, cyber warfare, etc. Like, hacking is institutionalized in China wherein virus writing is taught in Chinese military schools.

• Enhance in-house technical research and development capabilities especially in relation to signals decryption work, and cryptography capabilities.

• Upgrade Open Source Intelligence (OSINT) capabilities such as use of advanced commercial search engines; upgrade offensive as well as defensive capabilities in cyber warfare.

• Human/robotic penetration amongst terrorist organizations is a useful tool. Human intelligence and electronic intelligence will have to be tuned to the maximum to penetrate terrorist groups and focus on building operational data that can be regularly shared with the police, paramilitary forces and others.

• Offensive and defensive cyber capabilities are as important for the nations to build as the nuclear capabilities. We will soon have only two types of nations – those with Cyber offensive and defensive capabilities and those without. Cyber
capabilities would soon assume the proportions of Comprehensive Test-Ban Treaty (CTBT) and would become points of negotiations between nations.

2. **Investment and Education for Cyber Security**

- We all know that habits form at an early age. It is for this very reason that we should teach Children basics of Cyber Security and Cyber Hygiene on a Mission mode in a PPP configuration much like in a NSS program.

- Cyber security requires investment in people and systems. India has an abundance of raw IT talent and the best can be channeled for this type of work.

- There is a school of thought that cyber security actually requires an entirely new framework to be understood. Harvard and MIT have been working to build the new discipline of “Cyber International Relations” for just this purpose. Our technology institutions like IITs, IISc and unique universities should significantly enhance their research on cyber security with an active participation from the Industry.

- Western countries on the forefront of defense have set up research units, started academic research innovation, and run full-scale cyber-attack rehearsals. So must India. To build a cadre of elite security technologists, we need to promote hardcore computer science education in our technical institutes of high caliber.
Cyber attack capabilities require a brilliant trained workforce of youth. Like other nations, talent development exercises must be conducted in large scale to catch them young almost out of school. This would foster hacking talent and get a large brigade of hackers into the system. Who besides the human talent would also develop “Bots” (web robot) that would act as software soldiers ready to attack or defend as needed.

**Challenges for Cyber Policing**

One of the possible solutions for countering the threats is by being visible in the public domain and creating greater awareness breaking the traditional masks of secrecy that surround the intelligence operations. This exercise of being present in the event dominating social media to garner support from the public and managing the social media through well-orchestrated planning would be the greatest challenge for police forces in the years to come. The social media has become ever so powerful today. Predicting cascade effects in social media and the ability to alter the outcome of such cascades and arrest them when needed or directing to them one’s own advantage requires the symbiotic convergence of not merely the technology and social sciences but also a very watchful monitoring. The Technologies underpinning social media should be used to the advantage of unifying people for national growth and security. This will form the major thrust of all intelligence activities and I am sure that the Kerala Police and cyber
security experts assembled here would strive to be in the forefront of this very soon.

**I wish to give three directions wherein our focus must lie**

Friends, with the exposure by Snowden that many of Government transactions, and even the activities of political organizations in India and in many countries are being snooped by the US, leaves us with a feeling that we need far more aggressive approach to cyber security. India should look at technologies that confine Indian transactions to be within its shores and use secure access and encryptions that make it impossible to snoop. Our missions abroad and our official on tour outside must be given a safe and secure information access not only when using wired networks but also while using wireless. This will call for focused research and development of developing secure systems in unsecure environments.

Indian capabilities in decryption today are far beyond what would make our Law enforcement agencies feel comfortable. Cryptanalysis is a very tough complex field but Indians are known to be very good in Theoretical Computer Science, mathematics and Number theory. A national campaign to develop the capability to break any encryption within a year of its introduction has to be started.

The third area that India should master is the Social Media Analytics. Use of social media has been increasing exponentially and it is believed that in India alone we will have 283 Million users by the year 2017, majority of them being from the younger
generation. Social media world over has been used for good and bad purposes, and by covert and overt social groups. Social media has become the most effective tool in peace disruptions and it has and/or suspected to have played a key role in events such as the Blackberry riots in London in 2011, the Delhi Rape protest, 2012, Muzzafarnagar riots, 2013, exodus of people North East origin, 2012 Libyan and Egyptian Riots, and so on. The analysis of tweets and their locations have helped the police to track the crowd movements and their mood. Social media is also an effective tool conflict management to bring people together to fight violence, for community outreach by the police and civil services, during disaster management, and in identifying crime and criminals. It has also become a tool for governments to reach out and understand the feedback of the people and creating flat democracies.

Social media has also been used in Arab Spring revolution, the Egyptian revolution and the Iranian revolution and in fact had been responsible for bringing the regimes down. Indian Police have in many places are using the social media for managing traffic and to interface with the public. Social media is also represented by 3Vs – very high volume, velocity and variety making it as a subject for Big Data. For a country to succeed in civil society, it is important that the social media and its big data analytics have to be mastered through high quality intense research. The future of cyber security and in fact the national security would be centered around Social Media.

**Conclusion**
Friends, I am sure each one of you as a great mission to counter all forms of cyber threats and ensure a safe world for all. Let me conclude with a prophetic and visionary saying of Maharishi Patanjali propounded in Yoga Sutra before 2200 years.

"When you are inspired by some great purpose, some extraordinary project, all your thoughts break their bounds. Your mind transcends limitations, your consciousness expands in every direction, and you find yourself in a new, great and wonderful world. Dormant forces, faculties and talents come alive, and you discover yourself to be a greater person by far than you ever dreamt yourself to be."

My best wishes to all the members present here success in their mission of making India and the world a place where all citizens feel safe and secure.

May God Bless you all.