"Artificial Intelligence is the science and engineering of making intelligent machines"
- John McCarthy, father of AI

1.0 Importance of Artificial Intelligence

Artificial Intelligence is the key technology area today, cutting across all domains of Engineering and Science and impacting all walks-of life and making transformational impact in day-to-day life: from digital assistants who can mimic human actions; to intelligent tutoring that can tailor lessons to meet a student’s individual cognitive needs; to autonomous driverless cars; to assist doctors in medical diagnoses and so on.

Eminent Scientist Alan Turing was the first to give a thought if a ‘Machine’ can imitate ‘Man’. Researchers like Marvin Minsky and Dean Edmonds, gaining inspirations from the experiments and experiences in their study field followed suit with Turing’s thought and kick started the research with the dream of seeing Machines perform Human actions. This thought on AI bloomed in 1950 and went through a hype cycle between 1950’s to 1980’s.

The term, “Artificial Intelligence” (AI) was coined in a proposal for a conference in 1955 by a Dartmouth professor, John McCarthy, to gather researchers and explore ways to make a machine that could reason like a human and that is capable of abstract thought, problem-solving and self-improvement. The possibility of an intelligent machine led to few other subsequent developments such as, Machine Learning, Natural Language Processing (NLP), Speaker Recognition and Speech to Text Processing, Image Processing and Computer Vision etc.

AI evolution has gone through various phase Viz., Artificial Narrow Intelligence (ANI), Artificial General Intelligence (AGI) and Artificial Super Intelligence (ASI) [2]. ANI is the first stage of the evolution of AI which is limited in scope with intelligence restricted to only one functional area. ANI is, for example, on par with an infant [2]. ANI basically uses Rule based Systems, Context Awareness and Retention, Domain Specific Expertise and Reasoning Machines.

The second stage, AGI, is at an advanced level: it covers more than one field like power of reasoning, problem solving and abstract thinking, which is mostly on par with adults. Self-aware systems are such examples of AGI. Pattern recognition and machine learning techniques and other reasoning techniques are used in this stage. Google’s Deep Learning project falls in this category. Finally in the last stage which is called ASI in which AI surpasses human intelligence across all fields. Singularity and Transcendence of human capabilities would be the best examples of ASI where ASI could lead to a massive expansion in human capability. The humans could connect our brains to each other allow us to share ideas, solve problems collectively, and even give others access to our dreams as observers or participants. Taking things a stage further, we might also transcend the limits of the human body and connect to other forms of intelligence on the planet – animals, plants, weather systems, and the natural environment [3].
The transition from the first to the second stage has taken a long time but it is believed that we are currently on the cusp of completing the transition to the second stage - AGI, in which the intelligence of machines can equal humans [4].

Artificial Intelligence Task Force was set up by Ministry of Commerce and Industry, Government of India. The AI Task Force was set up to prepare India for the upcoming Industrial Revolution 4.0 and the resulting economic transformation, with an emphasis on artificial intelligence.

NITI Aayog unveiled its discussion paper [1] on national strategy on AI which aims to guide research and development in new and emerging technologies. NITI Aayog has identified five sectors - healthcare, agriculture, education, smart cities and infrastructure and transportation to focus its efforts towards implementation of AI. The paper focuses on how India can leverage the AI to ensure social and inclusive growth.

Ministry of Electronics & IT (MeitY), GoI had constituted four committees in February, 2018 with an aim of understanding various regulatory and technical challenges associated with AI along with areas where the technology could be implemented.

The present effort by SETS through this brainstorming session is to focus on AI and Cyber security keeping in view of its strengths in Information Security & Cryptology.

AI techniques could be used to improve and provide state of the art cyber security solutions on one hand, the AI systems themselves with remote monitoring and control through the Internet/Intranet systems cannot escape the cyber attacks and it is expected that the impact would be quite serious. The following section explains the issues of cyber security.

2.0 Growing Issues of Cyber Security

Cyberspace has united distinct information structures ranging from our business and government operations, our sensitive communications and transactions, our critical digital control systems and infrastructures. Hence Cyberspace protection is quintessential for making nation’s critical infrastructure and key resources resilient and reliable as they can cause huge loss in terms of money, time and reputation. Unfortunately cyber attacks have become a modern weapon of 21st century. The year 2017 would be remembered as the year of ransomware as we witnessed the worst ransomware attack ever mounted through a malware called Wannacry which infected more than 300,000 computer systems in just four days. Wannacry is followed by its ransomware variant called Petya affecting the country badly in the Asian pacific region as per the Symantec’s analysis. According to India’s Computer Emergency Response Team (CERT-in) [5] there were 49455, 50362 and 27482 cyber security incidents reported in India during the years 2015, 2016 and 2017(till June) respectively. The network security incidents include phishing, website intrusions and defacements, virus and denial of service attacks amongst others. A cyber attack on critical infrastructure could be worse than a war as it can cripple a nation [6] without firing a single shot.

Research community has been trying to address these network security problems for more than two decades by placing a significant emphasis on developing tools and techniques such as anti-virus software and Intrusion Detection Systems (IDS). Whenever an intelligent solution is proposed to resolve a network vulnerability, the attackers bring forth a smarter way to circumvent the proposed countermeasure. Hence the current security approaches may be effective against novice attackers using popular and known attack techniques; they become ineffective against attackers devising novel techniques and methodologies that render the security tools inadequate. Thus it is more challenging to secure the local network which is typically connected to the Internet whose major parts are beyond the control of network administrators. Due to the increased complexity of the communication and
networking infrastructure cyber-crimes prevention is becoming difficult and therefore new approaches such as AI techniques for cyber security are aspired. The next section explains the influence of AI on cyber security solutions and vice-versa.

3.0 Artificial Intelligence and Cyber Security

Whoever controls and leads in AI will rule the world.
- Nation State Leaders

AI is changing the game for cyber security, analysing massive quantities of risk data, to speed-up response times and augment the capabilities of under-resourced security operations. AI technologies like machine learning, deep learning and natural language processing enable analysis to respond to threats with greater confidence and speed. Organizations (business enterprises, Government, defence), are already beginning to use AI to bolster cyber security and offer more protections against sophisticated hackers. AI helps by automating complex processes for detecting attacks and reacting to breaches. These applications are becoming more and more sophisticated as AI is deployed for security.

In the context of cyber security, AI is able to perceive its own environment well enough that it can independently identify threats and take the appropriate action, all without the need for human intervention. AI is particularly powerful from an incident-response perspective because it is adept at recognizing patterns and anomalies far better than any human agent ever could.

Simply put, as the amount of data continues to grow and the global threat landscape continues to advance, both in number and sophistication of attackers, organizations can no longer rely on antiquated tools and manual activities.

Automated cyber security incident response powered by AI and machine learning will enable strategic organizations, business’ to stay a step ahead of the threats. But the challenge is not enough data and not enough expertise available to take benefit of ML, DL algorithms to mechanize human intelligence.

Intelligent automation is capable of quickly detecting and identifying not only known but also entirely new classes of threats. Over time, these systems will continue to learn, adapt and improve on their own, becoming even more effective at managing incidents and analyzing the changing behaviours of attackers. Additionally, deep learning algorithms will be able to sift through enormous amounts of data in real-time to uncover valuable insights into the growing threat landscape, enabling rapid and effective improvements to existing incident remediation processes. Attackers are beginning to deploy AI too, enabling it to have the ability to make decisions that benefit attackers. Meaning they will gradually develop automated hacks that are able to study and learn about the systems they target, and identify vulnerabilities, on the fly.

The protection of AI systems, their data, and their communications is critical for users’ safety and privacy, as well as for protecting the eco-system. AI and Security are proving to go hand in hand in enabling delivery of positive outcomes of the implemented technologies.

As it is conceptualized, Cyber Security enables better AI by enhancing the Integrity (like by using adversarial machine learning techniques) and producing accurate results, maintaining Privacy of sensitive data of users (secure, privacy preserving machine learning) & preventing misuse of AI technology.

On the other hand Artificial Intelligence enables Cyber Security applications and plays a major role in the cyber security domain. By the integration of AI into the Security systems, the fast evolving cyber attacks facing global businesses can be to a large extent identified and arrested.
AI and Cyber Security enables and complements each other to make system to work better and more safely and efficiently.

AI enables new cyber security capabilities whereas cyber security enables a better AI and also prevents misuse of AI [7].

Intersection of Figure shows how will Cyber (in)security impact the development of AI and how the rise of AI will alter the security landscape.

**Figure: AI and Cyber Security**

Cyber security in context of AI is looked at as two different implementations:

Firstly, **Cyber Security for AI** – The focus has to be on the protection of compute, data and algorithm. AI solutions are getting widely deployed today and Security must be an important consideration as those solutions evolve.

Second implementation is **AI for Cyber Security** – To use AI for the detection of Advanced exploits. This implementation is very important and has lot of potential though yet in embryonic state. Industries are to be encouraged to gear up and play a major role to manage the expectations of this implementation.

### 3.1 Artificial Intelligence for Cyber Security

"Advanced AI learns to understand cyber security, recognize patterns and connect dots between threats" 

- Jeb Linton, Chief Security Architect, IBM Watson

AI is supposed to be very compatible technology to drive efficient cyber security services. AI enabled cyber security provides two major classes of benefits: cyber security functions can be improved tremendously and, cyber security risks can also be minimized at the same time. Following are some of the advantages of using AI technology in the cyber security applications:

**i. Scaling resistance to counter cyber attacks**

AI based security applications can read and understand security very sensitively and therefore they have the potential to increase the scale of resistance such that the system can handle the ongoing attacks very efficiently. The cyber-assault can target a huge number of devices and software in an organization which can be well responded by AI based solutions through automated or robotic programs. The Artificial Intelligence based mechanisms can be deployed to take counter-measures in real time.

**ii. Countering zero day attacks**

AI based systems can analyse incidents very efficiently and can identify their root causes. They can also find out the methods that were used to deploy such incidents and can learn the trends smartly. Hence they can predict the next pattern of incidents even before they really take place. Such attacks are known as zero day attacks and can be detected well in advance using AI based techniques.
iii. Fast learning from big data set
The legacy or traditional cyber security applications cannot manage real time responses to the cyber-attacks due to having voluminous data set in hand and speed issues concerned with them. They become unable to analyse the data along with the shifting nature of the attack itself and therefore, cannot formulate a response and due course of actions to prevent or mitigate them. Such difficulties arise because no automation in their cyber-threat response mechanisms is in place.
AI enables cyber security to focus on relevant signals in the voluminous data set based on situational awareness. Thus AI based systems are extremely fast learner as compared to human security analyst.

iv. Quick reaction to a range of threats
We are today in a stage to defend zero-day attacks or unknown attacks which are on the way to our network. We have still not achieved the optimal balance of false positive and false negative alarms for intrusion detection over the network. Use of AI in such scenario helps us to dynamically react to a range of threats and gain optimal balance of false positive and false negative alarms for intrusion detection over a network.

v. Countering threats in real time
AI enables counter-measures against a threat in real time. For example, AI based security applications achieves the optimal balance of false positive and false negative alarms for intrusion detection over the network in real time.

vi. Anti-gaming Capabilities
AI based systems can enable anti-gaming capabilities to defend itself from unusual behaviour of a server equipped with gaming capabilities. Also, AI enabled servers can apply Anti-gaming capabilities to an attacking server as an Offensive Defence Strategy.

vii. Malware Analysis
Malwares are inserted into computer networks with malicious intention, causing heavy damage to resources. Advanced techniques like code obfuscation make detection and analysis of such malware highly difficult. Machine learning techniques like hidden Markov model and deep learning are being used to model malware behaviour. Highly parallelizable codes based on ML techniques, running on GPUs are being used to provide defence against malware infection. On the other hand, ML techniques are being used to design more and more complicated malware, which are getting harder to find.

viii. Natural Language Processing
The field of Natural Language Processing focusses on the interactions between human language and computers. It draws techniques from computer science, machine learning and computational linguistics. The outcome of NLP could be automatic summarization, translation, named entity recognition, relationship extraction, sentiment analysis, topic segmentation and speech recognition. NLP operates by automatically learning rules of the knowledge using machine learning techniques and making statistical inference. Social media and Rich Site Summary (RSS) analysis are often quoted as use cases for NLP.

ix. AI for national requirements of security
AI can also be used for current and future implementation in Cyber Security through Offensive and Defensive Measures as per current national security requirements.

x. Cyber Courses of Action (COAs)
AI can benefit cyber security through the use of automated techniques to generate cyber courses of action (COAs) in response to cyber threats.

This section discussed on how AI enables cyber security and in the following section we touch upon briefly the need of securing AI systems.
3.2 Cyber Security for Artificial Intelligence

Use of AI based applications and systems are growing day-by-day making them an attractive target for the attackers. Attackers may be able to exploit weaknesses in AI systems through very subtle means. Simple, small and often undetectable alterations in content including images, video, and audio recordings can be crafted to confuse AI systems, even without a deep knowledge of the AI a cyberattack is targeting. Following are the two main goals of attackers while targeting AI based systems [7]:

(i) Attack on AI Systems
Most of the attacks on AI systems generally cause learning system not to produce intended or correct results; or cause the learning system to produce the targeted outcome desired by the attacker and also to obtain sensitive information about the individuals. The above problem can be addressed by securing the learning systems of AI.

(ii) Misuse of AI
Attackers try to misuse AI to attack other systems. They find vulnerabilities in other systems and target attacks or devise attacks. In such cases we need to secure other systems.

The goals of the creator/designer and the AI system must be aligned in order to avoid any unexpected behaviour from the AI system which may develop destructive methods to achieve its goals. For example, in Tesla car accident, the vehicle mistook a white truck for a clear sky, offers an example of an AI misunderstanding its surrounding and taking deadly action as a result.

Securing AI systems using traditional cyber security solutions at various levels in the design of AI based applications is of paramount importance. Some of such security features are given below:

a. Verifiable Security
A robot or software program or any other AI system must be ensured to remain verifiably safe throughout its lifetime, even as it continues to learn and develop on its own. We need to set a level up-to which we can accept loss in order to gain the potential benefits of AI based super intelligent systems. One way to achieve verifiable security in the AI systems is to make AI based products to be safe from start to finish. This essentially requires that there should not be any black box implementation in the AI based systems.

In case of development of super-intelligent systems, we need to quantify a mark upto which a loss can be tolerated in order to gain its potential benefits. They must also be designed to be resistant to cyber-attacks, in their own right, with some kind of verification and validation measures in place, to confirm their continued usability, in the event of an assault [8].

b. Security enabled Design
Designing smarter AI systems is a cognitive task. Proactive measures are important in the design of a secure AI based systems. Designing super-intelligent machines must incorporate proactive measures to prevent them to make bad decisions leading to fatal effects on human lives. The design of super-intelligent machines must guarantee strict adherence to the designer’s goals.

c. Privacy Preserving
AI systems should be designed in such a way that privacy of an individual or organization is safe throughout dealing with the large volume of data sets. There should be effective methods which can ensure privacy of the individual in AI enabled applications.
4.0 Standards for developing AI Systems

As AI technologies become more widespread, efforts to ensure that they work as intended become more critical. If humans are to trust AI, cyber security of AI-fuelled systems must be based on standardized and audited operations. Data being the key to the AI security it is necessary to use standard formats for data or meta data to ensure interoperability. AI should engage in performing robust self-audit and ensure that security by design principles are in place. As AI being the next generation technology influencing in all walks of our lives, it should be therefore, trustworthy as far as its designer’s motives are concerned. AI systems typically make decisions based on data-driven models created by machine learning, or the system’s ability to detect and derive patterns. As the technology advances, we will need to develop rigorous scientific testing that ensures secure, trustworthy and safe AI. We also need to develop a broad spectrum of standards for AI data, performance, interoperability, usability, security and privacy.

5.0 Intent of the Meet and Points for Discussion

The growing importance of use of AI based solutions in different domains and the related security challenges and also the use of AI techniques in providing advanced security solutions in securing networks, systems, end systems as explained above needs an open discussion at various levels and with the experts working in this direction. It is proposed to invite few of the experts from academic institutes, industry and R&D labs to discuss on some of the challenges posed in this area of National interest and how to tackle and arrive at solutions. Some of the technology areas (but not limited to) where AI could be used for providing effective cyber security solutions are listed below:

i. Next generation Intrusion Detection and Prevention System (IDPS) that integrates automatic agents for detection, analysis and prevention.

ii. Automatic Verification of Software can integrate AI Agents to prove theorems and verify programs.

iii. AI based DoS Mitigation Application

Development of AI based DoS Mitigation Application which can integrate anti-gaming approach to spoof adversaries equipped with gaming capabilities.

iv. Deep Learning for vulnerability in IoT Devices

Development of security software to automatic vulnerability detection and patching.

v. AI for Hardware security

a. Security solution based on power analysis and Artificial Intelligence (AI) called Power Fingerprinting (PFP) with a focus on protecting chip integrity.

b. Using Artificial Intelligence (AI) to Detect Hardware Trojan (HT)

c. Use of Artificial intelligence (AI) technologies to accurately detect which wires in an IC make up a hardware Trojan.

The main purpose of the AI and Security discussion meet is to bring together AI and cyber security experts, to see the existing strengths and identify gap areas and the thrust areas to focus. It is also expected to chart-out future course of action and to suggest possible collaborations in order to arrive at usable solutions at national level for AI and Security.
The following are the proposed points of discussion during the meet:

1. Which areas of cyber security can be strengthened using AI techniques?
2. What e-security measures need to be enforced for securing AI systems?
3. Which R&D areas need to be focussed with the aim of cyber security solution development using AI? Evaluate expertise available in the country and identify gap areas.
4. What are the mechanisms for policy framing, standards implementation and testing in this domain?
5. Plan of action - Way forward

6.0 Conclusion

Based on the above aspects of AI and Cyber security and their impact on various solutions/ products which would go into different domains, including cyber physical systems and critical infrastructure, it is proposed to have a meeting with experts to discuss the issues, challenges and to arrive at an approach to understand and arrive at a plan of action in carrying out research to provide solutions.

“We had better be quite sure that the purpose we put into the machine is the purpose which we really desire”
Norbert Wiener, 1960 (American mathematician and philosopher, originator of cybernetics)

References

2. Nores Automation and Robotics.pdf