PLUTUS IAS

CURRENT AFFAIRS

Argasia Education PVT. Ltd. (GST NO.-09AAPCAI478E1ZH)
Address: Basement C59 Noida, opposite to Priyagold Building gate, Sector 02,
Pocket I, Noida, Uttar Pradesh, 201301, CONTACT NO:-8448440231

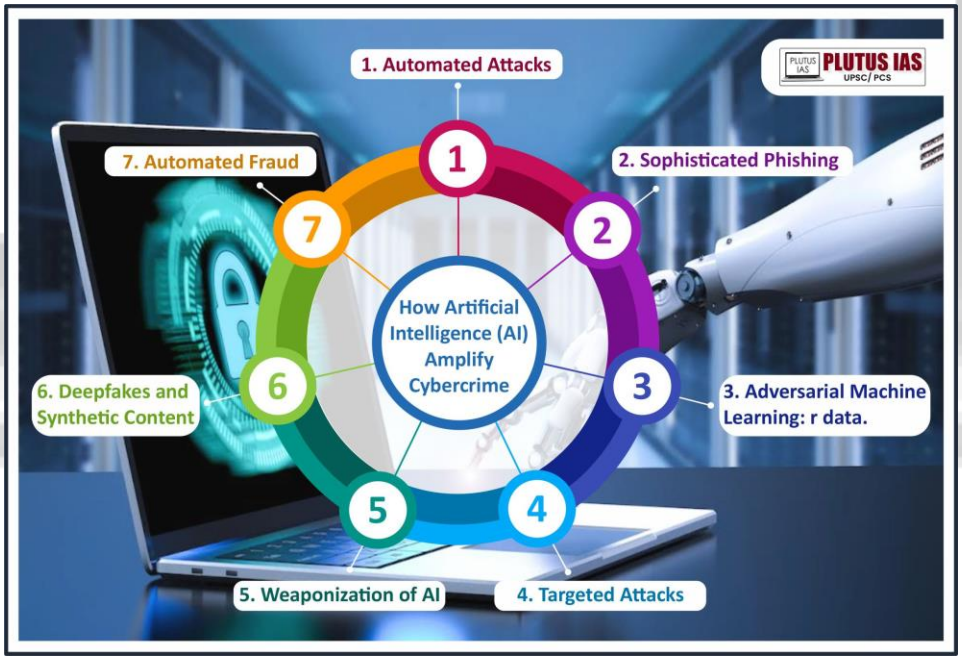
Date – 10 May 2024

CYBER SECURITY THREAT POSED BY ARTIFICIAL INTELLIGENCE

CONTEXT

The widespread integration of generative AI across various sectors like education, finance, healthcare, and manufacturing has indeed revolutionized our operations. However, it has also ushered in a new era of cyber risks and safety concerns. With the generative AI industry poised to boost the global GDP by a substantial $7 to $10 trillion, the proliferation of AI solutions (such as ChatGPT introduced in November 2022) has set off a complex interplay of benefits and drawbacks.

As per a study conducted by Deep Instinct, around **75% of professionals witnessed an upsurge in cyberattacks** in the past year alone, while 85% of the surveyed respondents have attributed the increased risk to generative AI.



A CASE IN US

In the recent past, there was a disturbing incident involving a distressed mother who received a terrifying call from individuals claiming to be kidnappers holding her daughter hostage. This event triggered significant concern within the U.S. Senate regarding the negative consequences of artificial intelligence. The nation was shaken as it became evident that the purported kidnappers and the voice of the daughter were actually the work of hackers employing generative AI to carry out their extortion

tactics. As these types of occurrences become more frequent, there is a growing erosion of human perception distinguishing between genuine reality and content generated by AI.

WHAT IS GENERATIVE AI?

Generative AI is a subset of artificial intelligence focused on creating or generating new content, such as images, text, audio, or video, that is indistinguishable from content created by humans. Unlike traditional AI systems that are designed for specific tasks or objectives, generative AI models are capable of generating diverse and original outputs based on the data they have been trained on.

Generative AI relies on advanced machine learning techniques, particularly deep learning, to understand and replicate patterns in data. These models can then generate new content by predicting and synthesizing patterns learned from the training data.

Some common examples of generative AI include:

1. **Text Generation:** Models like OpenAI's GPT (Generative Pre-trained Transformer) series can generate coherent and contextually relevant text based on a given prompt or input.
2. **Image Generation:** Generative Adversarial Networks (GANs) are a popular technique for generating realistic images. GANs consist of two neural networks, a generator and a discriminator, which are trained together in a competitive manner to produce high-quality images.
3. **Audio Generation:** Generative AI models can also generate realistic-sounding audio, including music, speech, or sound effects. These models are trained on large datasets of audio recordings to learn the nuances of human speech and music composition.
4. **Video Generation:** Similar to image generation, generative AI techniques can be used to create synthetic videos. These models can generate realistic video sequences based on input parameters or generate entirely new video content.

HOW AI CAN AMPLIFY CYBERCRIMES

Artificial intelligence (AI) has the potential to amplify cybercrime in several ways:

1. **Automated Attacks:** AI can be used to automate various stages of cyber attacks, from reconnaissance and scanning for vulnerabilities to launching exploits and spreading malware. This automation allows cybercriminals to scale their operations and target a larger number of victims more efficiently.
2. **Sophisticated Phishing:** AI-powered algorithms can analyze vast amounts of data to create highly personalized and convincing phishing emails or messages. These messages can mimic the writing style of the target individual or appear to come from trusted sources, making them more likely to deceive recipients and facilitate successful attacks.
3. **Adversarial Machine Learning:** Cybercriminals can exploit weaknesses in AI systems themselves. Through techniques like adversarial machine learning, attackers can manipulate AI models to produce incorrect outputs or evade detection, enabling them to bypass security measures and gain unauthorized access to systems or data.
4. **Targeted Attacks:** AI can be leveraged to analyze massive datasets and identify potential targets for cyber attacks with greater precision. This targeted approach allows cybercriminals to tailor their attacks to specific individuals, organizations, or industries, increasing the likelihood of success and maximizing the impact of their efforts.

5. **Weaponization of AI:** AI technologies such as machine learning algorithms can be weaponized to enhance the capabilities of malware and other malicious tools. For example, AI can be used to develop malware that can adapt its behavior in real-time to evade detection by traditional security solutions, making it more challenging to defend against.
6. **Deep Fakes and Synthetic Content:** AI-generated deep fakes and synthetic media can be used to create convincing but entirely fabricated images, audio, and video content. Cybercriminals can use this technology to impersonate individuals or manipulate media to spread disinformation, discredit individuals or organizations, or coerce victims into taking certain actions.
7. **Automated Fraud:** AI-powered fraud detection systems can also be exploited by cybercriminals. By understanding how these systems operate, attackers can design fraudulent activities to evade detection or manipulate the algorithms to approve malicious transactions.

WHAT SHOULD BE THE WAY FORWARD

1. **Develop Advanced Detection Techniques:** Invest in research and development of advanced detection methods specifically tailored to identify AI-generated content and distinguish it from genuine human-created content. This may involve leveraging AI itself, such as developing counter-AI algorithms capable of detecting and flagging suspicious or manipulated content.
2. **Enhance Education and Awareness:** Educate individuals and organizations about the existence and potential dangers of AI-generated content, including deepfakes and synthetic media. Increasing awareness can help people recognize and critically evaluate potentially deceptive content, reducing the likelihood of falling victim to AI-driven cyber threats.
3. **Strengthen Regulations and Standards:** Implement and enforce regulations and standards governing the use of generative AI technologies in cybersecurity and other domains. This may involve requiring transparency and accountability from AI developers, establishing guidelines for ethical AI usage, and imposing penalties for malicious activities involving AI-generated content.
4. **Promote Responsible AI Development:** Encourage responsible development and deployment of generative AI technologies by AI developers, researchers, and companies. This includes prioritizing ethical considerations, conducting thorough risk assessments, and implementing safeguards to prevent misuse or abuse of AI systems.
5. **Foster Collaboration and Information Sharing:** Facilitate collaboration and information sharing among government agencies, cybersecurity experts, AI developers, and other stakeholders to collectively address the challenges posed by AI-driven cyber threats. Sharing best practices, threat intelligence, and resources can help develop effective countermeasures and responses to emerging threats.
6. **Invest in AI Security Solutions:** Allocate resources towards developing and deploying AI-driven security solutions capable of detecting and mitigating AI-generated cyber threats in real-time. This may involve integrating AI into existing cybersecurity tools and systems to enhance their effectiveness against evolving threats.
7. **Promote digital Literacy and Critical Thinking:** Educate the public about media literacy and critical thinking skills to help individuals identify and evaluate the authenticity of information, regardless of whether it is generated by AI or created by humans. Encouraging skepticism and promoting fact-checking can empower individuals to navigate an increasingly complex media landscape.

Overall, while AI offers numerous benefits, its increasing sophistication also presents significant challenges for cybersecurity. As cybercriminals continue to leverage AI-driven techniques and tools,

organizations and security professionals must remain vigilant and continuously adapt their defenses to mitigate evolving threats.

Ankit Kumar

OLD TRADE ROUTE UNCOVERED BY INSCRIPTION AT HOYSALA'S TEMPLE

THIS ARTICLE COVERS 'DAILY CURRENT AFFAIRS' AND THE TOPIC DETAILS OF "OLD TRADE ROUTE UNCOVERED BY INSCRIPTION AT HOYSALA'S TEMPLE". THIS TOPIC IS RELEVANT IN THE "HISTORY" SECTION OF THE UPSC CSE EXAM.

WHY IN THE NEWS?

Inscriptions uncovered at the Sri Madhava Perumal Temple reveal evidence of a significant trade pathway existing over a millennium ago, linking the Kongu area in the western part of Tamil Nadu with southern Karnataka and Kerala.

ABOUT THE MADHAVA PERUMAL TEMPLE

- The Sri Madhava Perumal Temple, **located in Mylapore, Chennai, Tamil Nadu**, is dedicated to the Hindu deity Vishnu, who is worshipped as Madhava Perumal. The temple, **constructed in the Dravidian style of architecture**, dates back to the Hoysala period and was built during the reign of King Veera Ballala III (1292-1343 CE).
- The Mylapore region came under the rule of the Hoysala dynasty, and the general of the Hoysala army, Dhandanayaka, constructed the Dandanayaka Fort 680 years ago, with the **temple built inside the Dandanayaka fort**. The area was later ruled by the Vijayanagara Empire and Tipu Sultan, and the Battle of Sathyamangalam (1790), during the Third Anglo-Mysore War (1790-1792), took place near the fort.
- The temple is believed to be the **birthplace of Peyalwar**, one of the first three of the twelve Alvar saints of the 6th-9th century CE. The **inscriptions found at the temple reveal the existence of a village named Thuravalur** and indicate that the area served as a crucial trade route, **allowing traders to cross the Bhavani and Moyar rivers** to reach Wayanad in Kerala and various places in Karnataka.
- The temple, largely **submerged in the water-spread area of the Bhavanisagar dam in Erode district**, became visible as the water level in the dam dipped. The construction of the Bhavanisagar dam in 1948 resulted in the relocation of nearby residents and the shifting of temple idols to new locations in 1953.
- The discovery of this **submerged temple and the associated trade route highlights the importance of preserving and studying such historical sites**, as they offer a window into the past and contribute to our understanding of the region's history and cultural heritage. The inscriptions found at the temple provide valuable insights into the trade activities and historical significance of the region during the Hoysala period and beyond.

ABOUT HOYSALA DYNASTY

- The Hoysala Empire emerged as a dominant force in southern India, originating from Kannadiga roots and governing a vast expanse of territory encompassing present-day Karnataka during the 10th to 14th centuries. Initially headquartered in Belur, the capital later shifted to Halebidu.
- Rooted in the Malenadu region of the Western Ghats, the Hoysala rulers strategically expanded their domain during the 12th century, capitalising on conflicts between the Western Chalukya Empire and the Kalachuris of Kalyani. They annexed territories in present-day Karnataka and fertile lands north of the Kaveri delta in Tamil Nadu.
- By the 13th century, their dominion extended across most of Karnataka, parts of northwestern Tamil Nadu, and sections of western Andhra Pradesh on the Deccan Plateau. Claiming descent from the Yadava lineage, the Hoysalas traced their legendary origins to Sala, also known as Poysala, who purportedly exhibited exceptional bravery by slaying a tiger, earning the moniker "Hoysala," meaning "the one who strikes."
- Although the legend of Sala's valour is more symbolic than historical, it became integral to the Hoysala identity. While scant documentation exists about their early history, the Hoysalas initially served as vassals to various larger South Indian empires like the Chalukyas and Cholas before gradually asserting their independence and establishing their kingdom.
- The apex of Hoysala's influence unfolded during the 12th and 13th centuries under the leadership of notable monarchs such as Vishnuvardhana, Ballala II, and Veera Ballala III. This era witnessed prolific temple construction, illustrating their patronage of art and culture. The distinctive Hoysala architectural style, characterised by intricate sculptures and finely detailed carvings, reached its pinnacle during this period, leaving an enduring legacy of artistic splendour in the region.

ABOUT HOYSALA TEMPLE ARCHITECTURE

- Hoysala temple architecture is renowned for its remarkable beauty, meticulous craftsmanship, and the skilful work of the artisans who constructed these temples. These architectural marvels, erected during the Hoysala era, hold profound cultural and historical importance in the southern regions of India.
- During their reign, the Hoysalas displayed a remarkable dedication to temple construction, erecting numerous temples devoted to Hindu deities such as Lord Shiva, Lord Vishnu, and various forms of the Goddess. Notably, many Hoysala temples feature a distinctive star-shaped ground plan, incorporating multiple symmetrically positioned shrines. Constructed primarily from soapstone, these temples allowed for intricate carvings and detailed embellishments.
- A defining characteristic of Hoysala architecture is the elaborate carvings that adorn virtually every surface of the temples. These carvings depict scenes from Hindu mythology, celestial entities, animals, intricate geometric patterns, and depictions of Lord Vishnu and Lord Shiva. Additionally, Hoysala temples boast unique architectural elements like the Makara Torana, ornate Mantapas, circular pillars adorned with sculpted figures, and sanctums categorised based on the number of shrines.
- Hoysala temples exhibit a fusion of architectural styles, drawing influences from Chola and Chalukya art traditions. Their distinguishing features include star-shaped layouts, abundant decorative carvings, and the prevalent use of soapstone as the primary construction material. These temples serve not only as architectural wonders but also as repositories of the Hoysala dynasty's cultural and historical legacy, showcasing minimal Indo-Aryan influence and a more pronounced impact of the Southern Indian architectural style.

SOME NOTABLE EXAMPLES OF HOYSALA TEMPLES

- **Chennakesava Temple, Belur:** Constructed in the 12th century during the reign of King Vishnuvardhana, the Chennakesava Temple in Belur is one of the most famous examples of Hoysala architecture. Known for its breathtakingly intricate carvings and sculptures, particularly the famous "Madanikas" or celestial nymphs, this temple is dedicated to Lord Vishnu.
- **Hoysaleswara Temple, Halebidu:** Built in the 12th century under the patronage of King Vishnuvardhana and his successors, the Hoysaleswara Temple is another iconic Hoysala temple. Dedicated to Lord Shiva, this temple is renowned for its exquisite sculptures, especially the friezes depicting scenes from the Hindu epics Ramayana and Mahabharata.
- **Kesava Temple, Somanathapura:** Constructed in the 13th century during the reign of King Narasimha III, the Kesava Temple in Somnathpur is a remarkable example of Hoysala temple architecture. Known for its intricate craftsmanship and well-preserved sculptures, this temple is dedicated to Lord Vishnu.
- **Lakshmi Devi Temple, Doddagaddavalli:** Dating back to the late 11th century, the Lakshmi Devi Temple in Doddagaddavalli is one of the earliest surviving examples of Hoysala architecture. This temple is notable for its compact yet elaborately decorated structure, featuring intricate carvings of deities and celestial beings.

PRELIMS PRACTISE QUESTIONS

Q1. What purpose does the Mandapa in a Dravida-style temple serve?
(a) Ritual bathing
(b) Offering prayers
(c) Community gatherings
(d) Housing priests

Answer: C

Q2. The Gopuram of a Dravida-style temple is usually adorned with:
(a) Stupas
(b) Minarets
(c) Depictions of deities and mythological scenes
(d) Buddhist symbols

Answer: C

MAINS PRACTISE QUESTION

Q1. Evaluate the role of the Hoysala dynasty in the development of temple architecture, focusing on their patronage of art and culture. How did the distinctive features of Hoysala temples contribute to the region's architectural legacy?

Himanshu Mishra