NEXT IAS

दैनिक संपादकीय विश्लेषण

विषय

मिथ्या सूचना, कृत्रिम बुद्धिमत्ता और डिजिटल युद्धक्षेत्र

www.nextias.com

मिथ्या सूचना, कृत्रिम बुद्धिमत्ता और डिजिटल युद्धक्षेत्र

पाठ्यक्रम: GS3/साइबर सुरक्षा; उभरती प्रौद्योगिकियों की चुनौतियाँ

संदर्भ

- मिथ्या सूचनाओं का बढ़ता क्षितिज, साइबर खतरों का लगातार विकसित होता परिदृश्य, कृत्रिम बुद्धिमत्ता (एआई) और इसके विभिन्न रूप, जिनमें जनरेटिव एआई और आर्टिफिशियल जनरल इंटेलिजेंस (एजीआई) शामिल हैं, पूरे विश्व में सुरक्षा विशेषज्ञों के लिए सुरक्षा खतरों और चिंताओं की नई लहर उत्पन्न कर रहे हैं।

परिचय

- वर्ष 2024 एक अशुभ संकेत लेकर आया है - नए सुरक्षा खतरों का अग्रदूत जो पूरे विश्व के देशों और संगठनों के प्रतिरोध की परीक्षा लेगा। इन खतरों के दो प्रमुख रूप सामने आए: कृत्रिम बुद्धिमत्ता का उदय और मिथ्या सूचना अभियानों का बढ़ता क्षितिज। साथ में, उन्होंने एक जटिल संपर्क व्यवस्था का निर्माण किया - **'साइबर चक्रव्यूह'** - जिससे सुरक्षा विशेषज्ञ जूझ रहे है।

मिथ्या सूचना के क्षेत्र में जनरेटिव एआई का उदय

- कृत्रिम बुद्धिमत्ता, अपने विभिन्न स्वरूपों में, वरदान और अभिशाप दोनों बन गया है। जनरेटिव एआई और आर्टिफिशियल जनरल इंटेलिजेंस (एजीआई) अविश्वसनीय प्रगति का संकल्प करते हैं, लेकिन वे भानुमती का पिटारा भी खोलते हैं।
  - AI के माध्यम से ग़लत सूचना को प्रसारित करना चिंताजनक रूप से आसान हो गया है। डीप फ़ेक - डिजिटल रूप से विरूपित किए गए वीडियो, ऑडियो या चित्र - अब हमारे डिजिटल परिदृश्य में व्यापक रूप से उपलब्ध हैं।
  - ये भ्रामक रचनाएँ वास्तविकता और मनगढ़ंत बातों के बीच की रेखा को धुंधला कर देती हैं, जिससे भ्रम और अराजकता पैदा होती है। सच्चाई प्रायः क्षति हो जाने के बाद ही सामने आती है।

- हाल के वर्षों में, जनरेटिव एआई ने जनता की राय को प्रभावित करने और असहमति को दबाने के लिए राज्य के प्रयासों को गति दी है। पूरे विश्व में सरकारों और राजनीतिक अभिकर्ताओं ने, चाहे उनका लोकतांत्रिक या निरंकुश झुकाव कुछ भी हो, भ्रामक सामग्री बनाने और प्रसारित करने के लिए एआई का इस्तेमाल किया है।
- **सुलभता और सामर्थ्य:** जनरेटिव एआई उपकरण अधिक सुलभ और सस्ते हो गए हैं। प्रौद्योगिकी का यह लोकतंत्रीकरण मिथ्या सूचना अभियानों में प्रवेश की बाधा को कम करता है।
  - अब ये उपकरण केवल अच्छी तरह से वित्तपोषित राज्य अभिकर्ताओं का ही क्षेत्र नहीं रह गए हैं, बल्कि ये गैर-राज्य अभिकर्ताओं और यहाँ तक कि व्यक्तियों सहित विभिन्न संस्थाओं की पहुँच में हैं।
- **स्वचालित सेंसरशिप:** एआई सरकारों को ऑनलाइन सेंसरशिप के अधिक सटीक और सूक्ष्म रूपों का संचालन करने में सक्षम बनाता है। स्वचालित प्रणालियाँ आलोचनात्मक सामग्री को तेज़ी से पहचान सकती हैं और उसका दमन कर सकती हैं, जिससे असहमतिपूर्ण आवाज़ों को सुनना मुश्किल हो जाता है।
  - परिणामस्वरूप, वैश्विक स्तर पर इंटरनेट स्वतंत्रता में गिरावट आई है, तथा 2023 फ्रीडम ऑन द नेट रिपोर्ट में इस गिरावट के लगातार 13वें वर्ष पर प्रकाश डाला गया है।
- **डीप फेक और विरूपित सामग्री:** एआई द्वारा निर्मित डीप फेक - यथार्थवादी लेकिन मनगढ़ंत वीडियो या चित्र - का उपयोग मिथ्या सूचना प्रसारित करने के लिए प्रयोग किया जाता है। उदाहरण के लिए:
  - वेनेजुएला के सरकारी मीडिया ने सरकार समर्थक बयानों को बढ़ावा देने के लिए गैर-मौजूद समाचार एंकरों के एआई-जनरेटेड वीडियो का इस्तेमाल किया।
  - संयुक्त राज्य अमेरिका में राजनीतिक नेताओं के छेड़छाड़ किये गए वीडियो और चित्र सोशल मीडिया पर प्रसारित हो रहे हैं, जिससे सत्य और कल्पना के बीच की रेखा और अधिक धुँधली हो गई है।

- **पुरानी रणनीतियाँ विद्यमान हैं:** यद्यपि जनरेटिव एआई एक शक्तिशाली उपकरण है, सरकारें पुरानी रणनीतियाँ अपनाना जारी रखती हैं। ऑनलाइन चर्चाओं को आकार देने में मानव और बॉट अभियानों का संयोजन अभी भी प्रभावी है।
    - 2023 में, कम से कम 47 सरकारों ने दुष्प्रचार फैलाने के लिए टिप्पणीकारों को तैनात किया, जो एक दशक पहले की संख्या से दोगुनी है।

रक्षा और धूर्तता में एआई की भूमिका

- दुष्प्रचार अभियानों के अलावा, एआई रक्षा और युद्ध में भी महत्त्वपूर्ण भूमिका निभाता है।
- **युद्ध के मैदान में धोखा देना :** युद्ध के मैदान में धोखा देने के लिए AI का इस्तेमाल हथियार के रूप में किया जा सकता है। इस खतरे का मुकाबला करने के लिए, उन्नत AI-आधारित पहचान उपकरण आवश्यक हैं।
    - मशीन लर्निंग एल्गोरिदम एआई-जनित धोखे के संकेत देने वाले पैटर्न की पहचान कर सकते हैं, साइबर हमलों या मिथ्या सूचना अभियानों को रोक सकते हैं।
- **गैर-सरकारी अभिकर्ता और एआई:** राज्य और गैर-सरकारी अभिकर्ताओं द्वारा एआई-सक्षम तकनीकों का उपयोग महत्त्वपूर्ण जानकारी प्रदान करता है। ड्रोन, साइबरस्पेस और व्यापक स्तर पर मिथ्या और भ्रामक सूचना अभियान सभी इस क्षेत्र में आते हैं।

केस स्टडी

- **ताइवान चुनाव और दुष्प्रचार का तूफान:** 2024 के प्रारंभ में, जब ताइवान अपने चुनावों की तैयारी कर रहा था, तब दुष्प्रचार पहले से ही व्याप्त था। फर्जी पोस्ट और छेड़छाड़ किए गए वीडियो ने अनिश्चितता का माहौल बना दिया। यद्यपि कुछ लोगों ने इसके लिए चीन को जिम्मेदार ठहराया, लेकिन वास्तविकता इससे कहीं अधिक अस्पष्ट थी।
    - एआई द्वारा संचालित मिथ्या सूचना अभियानों को उर्वर भूमि मिल गई है। प्रामाणिकता के आवरण ने तथ्य और कल्पना में अंतर करना कठिन बना दिया है। जैसे-जैसे हम इस डिजिटल युग में आगे बढ़ रहे हैं, हमें यह पहचानना होगा कि एआई द्वारा संचालित मिथ्या सूचना हमारे समाज के लिए एक बड़ा खतरा है।

- **यूक्रेन संघर्ष:** यूक्रेन संघर्ष एक वास्तविक केस स्टडी के रूप में हमारे समक्ष विद्यमान है। जारी संघर्ष में, दोनों पक्ष एक दूसरे के विरुद्ध मिथ्या सूचना का उपयोग कर रहे हैं - जिसमें AI-सक्षम व्यवधान भी शामिल है। इसके परिणाम भयंकर हैं। भ्रामक कथाएँ, मनगढ़ंत साक्ष्य और विरूपित मीडिया संघर्ष की आग को हवा देती है।
    - डिजिटल युद्धक्षेत्र भौतिक युद्धक्षेत्र को बढ़ाता है, जिससे सत्य काल्पनिक हो जाता है। यह विश्व के लिए एक चेतावनी है: मिथ्या सूचना, जब एआई के साथ संयोजन करती है, तब स्थिरता और सुरक्षा को व्यापक क्षति पहुँचा सकती है।
- **सतत सतर्कता:** जुलाई-अगस्त 2024, फ्रांस में आयोजित 33वें ग्रीष्मकालीन ओलंपिक खेल डिजिटल हमलों का मुख्य लक्ष्य था। सुरक्षा विशेषज्ञों ने अभूतपूर्व खतरों के लिए स्वयं को तैयार कर लिया। सौभाग्य से, खेल बिना किसी बड़ी दुर्घटना के संपन्न हुए, जो उनकी सतर्कता का प्रमाण है।
    - लेकिन आत्मसंतुष्टि कोई विकल्प नहीं है। डिजिटल खतरों के नए-नए रूप सामने आएँगे, जिनके लिए निरंतर सतर्कता की आवश्यकता होगी। राष्ट्रीय सुरक्षा खतरे में है, और हमारी सुरक्षा व्यवस्था को उसी के अनुरूप परिवर्तित होना होगा।

साइबर अराजकता का पूर्वावलोकन

- हाल ही में, विश्व ने एक बड़े साइबर हमले के दौरान क्या संभव है, इसका अनुभव किया। हालाँकि यह जानबूझकर किया गया हमला नहीं था, लेकिन माइक्रोसॉफ्ट विंडोज अपडेट से जुड़ी एक सॉफ्टवेयर गड़बड़ी ने व्यापक व्यवधान पैदा कर दिया।
    - प्रारंभ में यह गड़बड़ी अमेरिका के कुछ भागों को प्रभावित करने के पश्चात्, भारत सहित पूरे विश्व में विस्तृत हो गई। उड़ान संचालन, हवाई यातायात नियंत्रण, स्टॉक एक्सचेंज और अन्य महत्त्वपूर्ण सेवाएँ बाधित हो गईं। भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-IN) ने इसे "गंभीर" घटना के रूप में वर्गीकृत किया।
- **वानाक्राई रैनसमवेयर (2017):** 150 देशों में 230,000 से अधिक कंप्यूटरों को संक्रमित किया गया; परिणामस्वरूप अरबों डॉलर की क्षति हुई।

- **शमून कंप्यूटर वायरस (2017):** एसए अरामको (सऊदी अरब) और रासगैस (कतर) जैसी तेल कंपनियों को निशाना बनाया गया; इसे 'इतिहास का सबसे बड़ा हैक' करार दिया गया; महत्त्वपूर्ण बुनियादी ढाँचे पर संभावित प्रभाव का प्रदर्शन किया गया।
- **पेट्या मैलवेयर (2017):** यूरोप, ब्रिटेन, अमेरिका और ऑस्ट्रेलिया में बैंकों, विद्युत् ग्रिडों और संस्थानों को गंभीर रूप से प्रभावित किया; वैश्विक प्रणालियों की परस्पर संबद्धता पर प्रकाश डाला।
- **स्टक्सनेट (2010):** ईरान के परमाणु कार्यक्रम को लक्ष्य करने वाला एक राज्य प्रायोजित वायरस; 200,000 से अधिक कंप्यूटरों को भौतिक रूप से क्षतिग्रस्त किया; लक्षित साइबर हथियारों की शक्ति का प्रदर्शन किया।

वैश्विक प्रयास

- **साइबरसिक्यूरिटी और इंफ्रास्ट्रक्चर सिक्यूरिटी एजेंसी (CISA):** यह वैश्विक साइबर सुरक्षा को मजबूत करने में महत्त्वपूर्ण भूमिका निभाती है। उनकी अंतर्राष्ट्रीय रणनीति, "CISA ग्लोबल", कई प्रमुख क्षेत्रों पर केंद्रित है:
  - **परिचालन सहयोग:** सर्वोत्तम प्रथाओं को साझा करने, सूचना के आदान-प्रदान में संलग्न होने और वैश्विक वितरण के लिए संयुक्त उत्पाद जारी करने के लिए समान विचारधारा वाले भागीदारों के साथ सहयोग करना।
  - **क्षमता निर्माण:** साइबर घटनाओं से बचाव और महत्त्वपूर्ण बुनियादी ढाँचे की सुरक्षा बढ़ाने के लिए अमेरिकी और वैश्विक क्षमता का निर्माण करना।
  - **हितधारक सहभागिता:** विभिन्न हितधारकों के साथ संपर्क और सहभागिता के माध्यम से सहयोग को मजबूत करना।
  - **नीति समर्थन:** साइबर और बुनियादी ढाँचे की सुरक्षा बढ़ाने के लिए वैश्विक नीति पारिस्थितिकी तंत्र को आकार देना।
- **वैश्विक सहयोग और मानदंड:** विशिष्ट एजेंसियों के अलावा, विश्व आर्थिक मंच (WEF) जैसे अंतर्राष्ट्रीय संगठन भी वैश्विक साइबर सुरक्षा प्रयासों में योगदान देते हैं। WEF चर्चाओं का आयोजन करता है, सर्वोत्तम प्रथाओं को साझा करता है, और सरकारों, व्यवसायों और नागरिक समाज के बीच सहयोग को प्रोत्साहित करता है।

- साइबरस्पेस में जिम्मेदार व्यवहार के मानदंड वैश्विक स्तर पर विकसित किए जा रहे हैं। इन मानदंडों का उद्देश्य डिजिटल क्षेत्र में राज्य के व्यवहार के लिए दिशा-निर्देश स्थापित करना है, जिम्मेदार आचरण पर जोर देना और दुर्भावनापूर्ण कार्यों को रोकना है।

भारत के प्रयास

- **भारतीय साइबर अपराध समन्वय केंद्र (I4C):** गृह मंत्रालय (एमएचए) ने साइबर अपराधों से व्यापक और समन्वित तरीके से निपटने के लिए कानून प्रवर्तन एजेंसियों (एलईए) के लिए एक ढाँचा और पारिस्थितिकी तंत्र प्रदान करने हेतु भारतीय साइबर अपराध समन्वय केंद्र (I4C) की स्थापना की।
  - साइबर अपराधों की रोकथाम और जाँच में I4C महत्त्वपूर्ण भूमिका निभाता है।
- **भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन):** सर्ट-इन एक राष्ट्रीय नोडल एजेंसी है जो साइबर सुरक्षा घटनाओं पर प्रतिक्रियाओं का समन्वय करने, प्रारंभिक चेतावनी और सलाह प्रदान करने तथा विभिन्न क्षेत्रों में साइबर सुरक्षा जागरूकता और क्षमता निर्माण पहल को बढ़ावा देने के लिए जिम्मेदार है।
- **साइबर स्वच्छता केंद्र (बॉटनेट स्वच्छता और मैलवेयर विश्लेषण केंद्र):** CERT-In द्वारा शुरू किए गए साइबर स्वच्छता केंद्र का उद्देश्य पूरे देश के कंप्यूटरों और उपकरणों से बॉटनेट और मैलवेयर संक्रमण का पता लगाना और उन्हें हटाना है।
  - यह उपयोगकर्ताओं को साइबर खतरों से अपने सिस्टम को सुरक्षित रखने के लिए निःशुल्क उपकरण और सेवाएँ प्रदान करता है।

- **साइबर फोरेंसिक सुविधाओं में सुधार:** सरकार मजबूत साइबर फोरेंसिक क्षमताओं के महत्त्व को पहचानती है। फोरेंसिक सुविधाओं को बेहतर बनाने के लिए निवेश किया गया है, जो जाँच के दौरान डिजिटल साक्ष्य का विश्लेषण करने में सहायता करते हैं।

निष्कर्ष और आगे की राह

- जैसे-जैसे AI विकसित होता जा रहा है, वैसे-वैसे सूचना युद्ध पर इसका प्रभाव भी बढ़ता जा रहा है। यद्यपि यह चुनौतियाँ प्रस्तुत करता है, यह स्केलेबल समाधानों के अवसर भी प्रदान

करता है। सही संतुलन बनाना - सामाजिक लाभ के लिए AI का लाभ उठाना और साथ ही इसके दुरुपयोग से सुरक्षा करना - इस डिजिटल युद्ध के मैदान में महत्त्वपूर्ण है।

- हमारा परस्पर जुड़ा विश्व सत्य, विश्वास और स्थिरता की रक्षा के लिए समन्वित प्रयासों की माँग करती है। और याद रखें, डिजिटल क्षेत्र में भी, सुरक्षा के लिए हमें सतत सतर्कता रहने की आवश्यकता होती है।
- साइबर सुरक्षा उपायों को मजबूत कर और साइबर खतरों के विरुद्ध अंतर्राष्ट्रीय सहयोग को बढ़ावा देकर इस 'साइबर चक्रव्यूह' से निपटने के लिए सूचित, सतर्क और सहयोगी होना महत्त्वपूर्ण है।

दैनिक मुख्य परीक्षा अभ्यास प्रश्न
[प्रश्न] आपके विचार में कृत्रिम बुद्धिमत्ता (एआई) का बढ़ता परिष्कार किस सीमा तक मिथ्या सूचना के प्रसार में वृद्धि कर रहा है, और सरकार एवं समाज इस बढ़ते खतरे का कितने प्रभावी ढंग से मुकाबला कर सकते हैं?

Source: TH