TENDÊNCIAS DE CIBERSEGURANÇA PARA 2025

Progress. Protected.

TABELA DE CONTEÚDOS

INTRODUÇÃO
3 — 4

1 **O IMPACTO DA INTELIGÊNCIA ARTIFICIAL GENERATIVA NA CIBERSEGURANÇA**
5 — 8

2 **OS DESAFIOS LEGAIS E ÉTICOS DO AVANÇO DA INTELIGÊNCIA ARTIFICIAL GENERATIVA**
9 — 12

3 **AS TECNOLOGIAS OPERACIONAIS (OTS) ESTÃO NA MIRA**
13 — 15

CONCLUSÃO
16

INTRODUÇÃO

É fundamental identificar as tendências que moldarão o mundo da cibersegurança em 2025 para garantir a prevenção, a detecção e uma resposta muito mais eficaz diante de novas ameaças cibernéticas. "Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas", diz um dos princípios-chave de A Arte da Guerra, de Sun Tzu. Aplicando esse conceito à cibersegurança, podemos dizer que "conheça a si mesmo" significa entender como toda a infraestrutura - em nuvem e on-premise - está protegida, identificar corretamente as vulnerabilidades aplicativas inerentes a cada uma delas e implementar planos de contingência que priorizem os ativos onde as informações são mais críticas.

Ano após ano, a informação se transformou em um tesouro cobiçado por cibercriminosos, tornando-se o novo ouro do século XXI. "Conheça o seu inimigo" significa compreender e estudar todas as táticas, técnicas e procedimentos (TTPs) que os cibercriminosos utilizam para se apoderar dessas informações.

No último *ESET Security Report 2024* apresentamos 12 dados sobre o estado da cibersegurança nas empresas da América Latina. O dado mais relevante do relatório é que 1 em cada 5 organizações sofreu pelo menos um incidente de segurança, sendo governo, tecnologia da informação e bancos/finanças os setores mais afetados. Além disso, 62% das organizações consideram que o orçamento destinado à cibersegurança é insuficiente, enquanto 28% indicaram que a cibersegurança é uma das principais preocupações.

Com esse cenário, os especialistas do Laboratório de Pesquisas da ESET América Latina analisaram **três tendências** que devem ser consideradas em 2025. Essas tendências, que já demonstraram um crescimento constante e uma relevância crescente em 2024, devem ter um impacto significativo na América Latina e continuar em evidência neste ano.
Para os responsáveis pela segurança da informação, o início de cada ano representa um desafio, pois os ativos tecnológicos possuem, geram e armazenam informações cada vez mais sensíveis de usuários e clientes. Por isso, é essencial criar ou atualizar políticas e estratégias que garantam a acessibilidade, integridade e disponibilidade desses dados.

A cibersegurança, afirmam os autores deste documento, deve ser uma prioridade estratégica para as altas direções das empresas ou instituições, onde o foco central deve ser uma participação transversal das áreas tecnológicas, operacionais, administrativas e de governança, que identifiquem os riscos cibernéticos aos quais estão expostos, tanto de forma específica quanto geral.

Uma das tendências identificadas é o **uso da Inteligência Artificial Generativa e das tecnologias emergentes**, cujo impacto vai além da simples automação de tarefas complexas e da análise de grandes volumes de dados. Assim como pode ser utilizada para detectar tráfego malicioso em tempo real e proporcionar uma resposta mais eficaz a um ciberataque, também seguirá a tendência de seu uso malicioso: a criação de campanhas de phishing muito mais sofisticadas e persuasivas dentro da engenharia social, o aprimoramento das deepfakes - e sua possível interação com a realidade virtual -, sem esquecer o desenvolvimento de malware polimórfico, capaz de driblar novos controles e tecnologias de segurança.

Outro aspecto desse crescimento exponencial da Inteligência Artificial Generativa e de sua capacidade de uso criminoso traz consigo a segunda tendência destacada neste documento: **os desafios legais e éticos que surgem com a utilização dessas tecnologias.**

Em nível global, e especialmente na América Latina, as normativas que abordam os problemas emergentes relacionados ao uso da Inteligência Artificial Generativa são insuficientes diante de um cenário de desenvolvi-

mento acelerado. As regulamentações existentes podem se tornar obsoletos ou desatualizados caso os avanços normativos não acompanhem esse ritmo.

Por fim, a terceira tendência destacada pelo Laboratório da ESET é o impacto do cibercrime em um setor que, muitas vezes, não recebe a devida atenção quando se trata de cibersegurança: os **Sistemas de Controle Industrial**, também conhecidos como Tecnologias Operacionais (OT, na sigla em inglês). A digitalização e a conectividade desses sistemas os tornaram alvos interessantes para os ciberataques.

Esses sistemas computacionais, que incluem diversos dispositivos, são utilizados para controlar processos industriais e físicos em diferentes setores, como energia, manufatura, abastecimento de água e gás, entre outros. Além disso, gerenciam equipamentos como PLCs (Controladores Lógicos Programáveis) e SCADA (Sistemas de Controle Supervisório e Aquisição de Dados), cujas funções principais incluem a automação de processos, o monitoramento e análise de operações, e a gestão de informações em ambientes produtivos.

Existem eventos históricos em que códigos maliciosos foram utilizados com o objetivo de vulnerabilizar esses sistemas. Um dos mais notáveis é o chamado "Aurora Generator Test", um teste realizado pelo governo dos Estados Unidos em 2007 que, pela primeira vez, demonstrou que um ciberataque poderia causar danos físicos a um gerador de energia. Outro exemplo muito mais recente é o ataque com os malwares BlackEnergy e *Industroyer* no qual a rede elétrica da Ucrânia foi comprometida em meio ao conflito com a Rússia.

À medida que a tecnologia avança, a exposição a ataques também aumenta, por isso é fundamental adotar uma abordagem de segurança baseada no conceito de confiança zero (Zero Trust). Em outras palavras, nenhum ativo tecnológico ou usuário pode ser confiável por padrão e, portanto, deve haver uma verificação contínua de sua identidade. Caso a identidade não seja verificada, devem ser tomadas as medidas adequadas para reduzir a superfície de ataque.

Não se trata apenas de implementar tecnologias de última geração ou abordagens para proteger a informação dos usuários, mas também é fundamental conscientizar e capacitar todos os níveis de uma organização sobre as boas práticas a serem seguidas. Isso significa oferecer aos usuários as ferramentas necessárias para identificar possíveis riscos cibernéticos, reduzindo, assim, as chances de um ciberataque.

A cibersegurança deve ser uma tarefa transversal em todas as áreas dentro de uma organização, pois estar ciente dessas tendências permitirá a atualização e o aprimoramento de políticas e tecnologias para enfrentar os desafios emergentes de 2025.

1

O IMPACTO DA INTELIGÊNCIA ARTIFICIAL GENERATIVA NA CIBERSEGURANÇA

Mario Micucci
Security Researcher na
ESET América Latina

A inteligência artificial generativa, representada por modelos avançados como o ChatGPT e o DALL-E, revolucionou a maneira como criamos, consumimos e entendemos a informação atualmente. Essa tecnologia, capaz de gerar textos, imagens, músicas e códigos de forma autônoma, promete transformar diversos setores. Na cibersegurança, ela não só oferece novas ferramentas para detectar, prevenir e responder a ameaças, mas também amplia os recursos de cibercriminosos.

Em um cenário onde os ciberataques se tornam cada vez mais sofisticados, a inteligência artificial generativa oferece soluções que permitem automatizar tarefas complexas, como a análise de grandes volumes de dados e a simulação de cenários de ataque. No entanto, essa mesma tecnologia também pode ser utilizada para criar campanhas de phishing mais convincentes, manipular modelos de IA, desenvolver malware polimórfico e amplificar o alcance das ameaças tradicionais.

Para os cibercriminosos, compreender como essa tecnologia está transformando as dinâmicas de defesa e ataque é fundamental. A chave será adotar uma abordagem equilibrada, explorando as oportunidades que a IA generativa oferece, enquanto se implementam medidas de proteção robustas para proteger as empresas e os usuários contra suas possíveis explorações.

A IA GENERATIVA A SERVIÇO DO CIBERCRIME

Embora já tenhamos visto as vantagens da inteligência artificial generativa no campo da cibersegurança, é importante destacar como uma tendência para 2025 o seu uso criminoso, que estimamos se intensificará nas seguintes áreas:

SPEAR-PHISHING AVANÇADO

Essencialmente, estamos falando da criação automatizada de e-mails e mensagens personalizadas com base na análise de dados públicos e privados, o que aumenta a eficácia dos ataques. A IA generativa pode analisar grandes volumes de dados, tanto públicos quanto privados, para criar mensagens altamente personalizadas e convincentes.

Ferramentas como o ChatGPT ou similares podem gerar mensagens que imitam perfeitamente o tom e estilo de comunicação de uma pessoa ou instituição. Por exemplo, ao obter dados de redes sociais, é possível gerar e-mails direcionados que mencionam eventos recentes ou temas sensíveis para a vítima.

Essas mensagens são praticamente indistinguíveis das legítimas, o que eleva significativamente a probabilidade de as vítimas clicarem em links maliciosos ou divulgarem informações confidenciais.

ROUBO DE IDENTIDADE

A criação de deepfakes para se passar por indivíduos em *videoconferências ou mensagens de voz utilizadas para fraudes ou extorsão* está em ascensão. A geração de vídeos e áudios falsos realistas (deepfakes) continuará sendo uma ferramenta usada para enganar indivíduos e organizações.

Com dados suficientes de áudio ou vídeo de uma pessoa (por exemplo, obtidos de redes sociais ou conferências públicas), a IA generativa pode criar conteúdo falso que imita sua voz ou aparência. Isso pode ser usado para convencer funcionários a transferir fundos ou acessar sistemas críticos.

As fraudes que antes eram realizadas por texto agora alcançarão um nível de realismo que dificultará sua detecção, mesmo por usuários treinados.

PROPAGAÇÃO DE DESINFORMAÇÃO:

Este ano, poderemos continuar observando o uso da IA generativa em diversas campanhas com o objetivo de desinformar ou distorcer a opinião pública. O uso em massa de textos, imagens e vídeos gerados por IA para manipular a percepção pública está se destacando como uma tendência, sobrecarregando as capacidades de verificação de fatos. A IA generativa permite criar e distribuir conteúdo falso de maneira massiva e altamente convincente.

Modelos de IA podem gerar artigos, imagens e vídeos que parecem autênticos. Isso inclui falsificar declarações de figuras públicas, criar notícias falsas ou manipular evidências visuais para sustentar falsas narrativas. Seu impacto é claro: mina a confiança pública nas instituições, afeta os processos democráticos e promove a polarização social. Na América Latina, esse tema tem *gerado crescente preocupação.*

CRIAÇÃO DE MALWARE

- Cada vez mais, observa-se a geração assistida de código malicioso mais sofisticado e ofuscado, aproveitando modelos avançados de IA para escapar das detecções. A IA generativa pode facilitar a escrita de código malicioso mais complexo e difícil de identificar.

- Modelos como o Codex podem sugerir estruturas de código otimizadas para burlar mecanismos de detecção, incluindo técnicas avançadas de ofuscação ou polimorfismo. Além disso, a IA pode automatizar testes para identificar vulnerabilidades nos sistemas.

- Isso acelera a velocidade e a sofisticação do desenvolvimento de malware, reduzindo as barreiras técnicas para cibercriminosos menos experientes.

AUTOMATIZAÇÃO DE ATAQUES

Se há algo que caracteriza cada vez mais o cibercrime, é a

automatização de suas tarefas. Com o uso de IA generativa, por exemplo, é possível realizar testes em larga escala em infraestruturas, buscando vulnerabilidades que possam ser exploradas. A IA generativa pode automatizar processos em ciberataques, desde o reconhecimento até a exploração de vulnerabilidades.

Recentemente, a OpenAI, empresa por trás do ChatGPT, *divulgou um relatório* detalhando como seus modelos de IA foram utilizados para realizar tarefas em fases intermediárias de ciberataques - depois da aquisição de algumas ferramentas básicas, mas antes da execução dos ataques, como campanhas de phishing ou distribuição de malware por diferentes meios.
No mesmo relatório, a empresa identificou que diferentes grupos APT (Ameaças Persistentes Avançadas) utilizaram a tecnologia para diversas finalidades, como depuração de código malicioso, pesquisa de vulnerabilidades críticas, aprimoramento de ataques de phishing, geração de imagens e comentários falsos, entre outras.

Além disso, o uso de bots impulsionados por IA pode ser empregado para rastrear continuamente redes e sistemas, buscando configurações incorretas, portas abertas ou softwares desatualizados. Uma vez identificada uma vulnerabilidade, esses bots podem gerar scripts de exploração específicos instantaneamente.

Isso amplia a escala dos ataques, permitindo que os cibercriminosos ataquem múltiplos alvos simultaneamente com um investimento mínimo.

ÁREAS DA CIBERSEGURANÇA IMPACTADAS PELA IA GENERATIVA

É um fato que a chegada da inteligência artificial generativa está marcando um antes e um depois na cibersegurança, afetando diversas áreas-chave de conhecimento e operação. Vamos analisar algumas das mais relevantes:

1. Defesa Cibernética Avançada

Os modelos de IA generativa estão revolucionando a forma como as organizações identificam e mitigam ameaças. Devido a sua capacidade de analisar padrões de comportamento em tempo real, essas ferramentas podem:

- Detectar ataques antes que causem prejuízos significativos, identificando anomalias em grandes volumes de dados de rede.

- Propor respostas automatizadas a incidentes, como bloqueios de IPs suspeitos ou ajustes dinâmicos nas configurações de firewall.

Por exemplo, um sistema baseado em IA generativa pode analisar o tráfego em tempo real, identificar um ataque DDoS emergente e implantar contramedidas em questão de segundos.

2. Simulação de Ameaças

A IA generativa facilita a criação de cenários hiper-realistas para testes de cibersegurança, permitindo que as organizações:

- Simulem ciberataques avançados para avaliar a resiliência de seus sistemas.

- Gerem ameaças hipotéticas com base em táticas emergentes de cibercriminosos, ajudando a desenvolver defesas preventivas.

Um exemplo é o uso de IA para gerar e-mails de phishing simulados adaptados ao perfil de um funcionário ou funcionária, treinando as equipes internas a reconhecer sinais de alerta.

3. Desenvolvimento de Capacidades Humanas

O treinamento em cibersegurança está se transformando com a IA generativa, permitindo:

- Criar conteúdo educativo personalizado para cada nível de usuário.

- Projetar cenários de treinamento dinâmicos, como simulações de ataques direcionadas a perfis específicos.

Por exemplo, organizações mais inovadoras já estão utilizando IA generativa para adaptar sessões de capacitação sobre phishing de acordo com o papel dos funcionários e funcionárias, maximizando o impacto e reduzindo lacunas de conhecimento.

4. Automação de Respostas Forenses

Em incidentes de segurança digital, o tempo é um fator crucial. A IA generativa pode desempenhar um papel fundamental para:

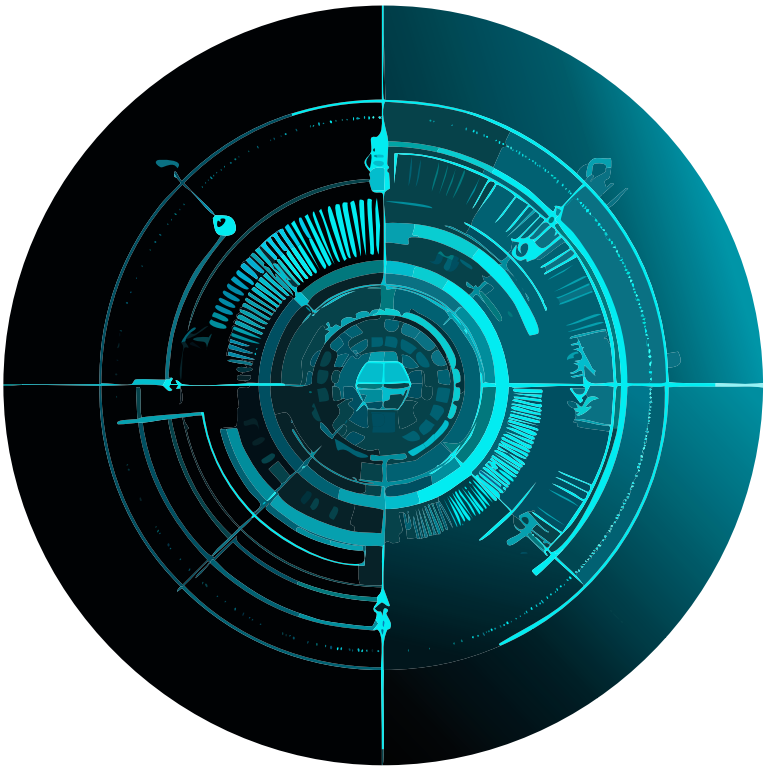
- Organizar e analisar grandes volumes de logs em busca de padrões que identifiquem a causa raiz de um ataque.
- Gerar relatórios detalhados com possíveis soluções e recomendações específicas para cada cenário.

Isso não apenas acelera a resposta a incidentes, mas também reduz a carga operacional das equipes forenses, permitindo que foquem em tarefas críticas.

Observar os detalhes dessas áreas mostra como a IA generativa não apenas amplia as capacidades defensivas, mas também redefine a forma como as organizações passam a pensar e agir diante dos desafios da cibersegurança. No entanto, não podemos ignorar que esse potencial vem acompanhado de desafios significativos.

Embora o uso da IA como ferramenta defensiva seja promissor, é fundamental considerar que os adversários também estão se beneficiando dessa tecnologia. Além disso, sua eficácia depende diretamente da qualidade dos dados com os quais é treinada e da robustez dos algoritmos utilizados. Nesse contexto, surgem várias questões que precisarão ser respondidas, como:

- Com que qualidade de dados os sistemas de IA estão sendo e serão treinados?
- Quem supervisiona e seleciona esses dados e de que forma?
- Que tipos de algoritmos estão sendo e serão utilizados para treinar esses sistemas?
- Sob quais critérios esses sistemas tomam e poderão tomar decisões?



2

OS DESAFIOS LEGAIS E ÉTICOS DO AVANÇO DA INTELIGÊNCIA ARTIFICIAL GENERATIVA

Fabiana Ramírez Cuenca
Security Researcher na
ESET América Latina

Diante do crescimento da inteligência artificial generativa e seu potencial uso malicioso, surgem desafios legais e éticos que, em sua maioria, ainda não foram adequadamente abordados. Quem é o responsável pelos atos da inteligência artificial? Quais limites deveriam ser impostos ao seu desenvolvimento? Qual organismo é competente para julgá-lo?

Atualmente, existem poucas normas internacionais que tratam das questões emergentes do uso da IA, e aquelas que existem muitas vezes são insuficientes diante do panorama de desenvolvimento acelerado dessa tecnologia.

De qualquer forma, durante este ano, é provável que a principal tendência nessas questões seja um maior escrutínio dos algoritmos e modelos de IA para garantir transparência e explicabilidade, além de regulamentações voltadas para a proteção de dados, a fim de assegurar a privacidade no uso da IA.

Veremos a busca por soluções para os prejuízos causados pela IA e a promoção, do ponto de vista regulatório, da ética no uso e desenvolvimento dessa tecnologia. Também continuarão os avanços nas regulamentações sobre cibersegurança aplicadas a essa temática e no campo da cooperação internacional.

A inteligência artificial, em suas diversas formas, nos trouxe uma grande quantidade de benefícios. Hoje em dia, contamos com diversos algoritmos de automação de processos, aplicáveis a diferentes áreas. Também podemos ver a IA no cotidiano, voltada para usuários comuns, com exemplos como assistentes de voz e IAs capazes de processar linguagem natural, como o ChatGPT, Gemini, Copilot e Meta AI, que são talvez as implementações mais conhecidas, mas não as únicas. E isso não é tudo: também observamos um grande crescimento no uso da IA Generativa em todas as suas formas, além de novas implementações na área da saúde, com o objetivo de melhorar diagnósticos e até mesmo sendo experimentada em cirurgias. Esses são apenas alguns dos muitos usos da IA atualmente.

No entanto, os algoritmos estão ao alcance de todos, existindo uma grande quantidade de fontes abertas de onde podem ser obtidos, personalizados e até utilizados para fins menos éticos, como a criação ou aperfeiçoamento de códigos maliciosos, geração de deepfakes e fake news, para citar os mais conhecidos.

Vale destacar que os algoritmos de IA não são intrinsecamente maliciosos; isso depende do uso que os humanos fazem deles. Esta tecnologia foi criada inicialmente para servir à humanidade, mas há aqueles que a implementam com fins ilícitos, o que demonstra o potencial da IA para causar prejuízos, muitas vezes devido ao seu uso intencional e, em outras ocasiões, devido a um desenvolvimento inseguro ou negligente dos algoritmos.

DESAFIOS NA IMPLEMENTAÇÃO DA IA

Se analisarmos a IA atual e seus usos, fica claro o motivo de sua implementação: facilitar a execução de diversas tarefas para os humanos, uma vez que os algoritmos são capazes de realizá-las de forma mais rápida e, muitas vezes, até mais precisa.

No entanto, no momento do desenvolvimento dos algoritmos e de seu uso posterior, inicialmente não se considerou como isso poderia afetar questões relacionadas aos direitos humanos. Vale destacar que isso também ocorreu com a maioria das tecnologias no início de sua implementação, e não é uma característica exclusiva da IA.

De fato, podemos mencionar alguns desafios relacionados a essa questão:

- **Privacidade de dados:**
Os modelos de IA são treinados com grandes quantidades de dados, o que já levanta questões sobre como esses dados são coletados, armazenados e utilizados, especialmente quando se trata de informações pessoais. No âmbito legal, os usuários devem consentir com a coleta e o tratamento de dados, mas, para que o consentimento seja válido, ele deve ser informado (o que significa que o usuário realmente compreenda todos os aspectos envolvidos). E é aqui que surge a dúvida: os usuários realmente compreendem como seus dados serão utilizados ou para quê? Além disso, a IA pode ser usada para rastrear, perfilar e monitorar pessoas em diferentes aspectos de suas vidas, o que levanta preocupações sobre a privacidade e até sobre a liberdade individual.

- **Qualidade dos dados:**
Os dados usados para treinar os modelos de IA podem conter vieses, o que pode levar a resultados discriminatórios ou injustos. De fato, a qualidade dos dados pode variar e afetar a precisão e confiabilidade dos resultados obtidos pelos modelos de IA. A qualidade implica que os dados atendam a características como precisão, integridade, consistência, relevância, atualidade, acessibilidade e veracidade.

- **Propriedade intelectual:**
Como os modelos são capazes de gerar conteúdo de diversos tipos, o que, é claro, fazem a partir dos dados com os quais foram treinados, surgem várias questões, como quem é o proprietário das obras geradas (se a empresa desenvolvedora ou o usuário que solicita a geração). Nesse contexto, também é importante questionar como as leis se aplicam ao conteúdo gerado pela IA e como seria possível detectar um plágio, ao menos parcial.

- **Transparência:**
Muitos algoritmos de IA, como os de Deep Learning, atingem um nível de complexidade que os torna difíceis de compreender, até mesmo para seus desenvolvedores, o que dificulta a avaliação de seu funcionamento. Isso pode levar à situação em que, em certos resultados, não seja possível explicar exatamente como a IA chegou a tais conclusões. É importante desenvolver modelos que sejam capazes de explicar como chegam às suas conclusões, uma vez que a informação é um direito dos cidadãos, e entender o processo de trabalho do modelo permitirá ajustá-lo, se necessário.

- **Manipulação da informação:**
A IA e sua grande capacidade generativa podem ser usadas para criar conteúdo falso, como vídeos ou áudios, além de ampliar a disseminação de fakenews. Muitas vezes, isso torna difícil distinguir o que é falso do que é real, permitindo que a tecnologia seja usada para desinformar e até manipular a opinião pública.

- **Uso vinculado às armas:**
Sabe-se que a IA também está sendo utilizada no âmbito militar, com experimentos envolvendo sistemas de armas autônomas que poderiam causar prejuízos à humanidade, caso não sejam estabelecidos limites claros.

- **Substituição laboral:**
A IA permite automatizar muitas tarefas, o que pode levar à perda de certos empregos por substituição. No entanto, considera-se que os seres humanos precisarão aprender a trabalhar com essa tecnologia, uma vez que as ofertas de trabalho irão variar, mas não diminuir. A automação pode, potencialmente, ampliar a desigualdade econômica, já que os benefícios da IA ficariam concentrados em um pequeno grupo de pessoas, e a especialização necessária para trabalhar com essa tecnologia seria mais acessível para setores com maiores rendas.

- **Segurança na implementação e desenvolvimento:**
Como todo sistema, os modelos de IA podem ser

vulneráveis a ataques cibernéticos, o que pode ter consequências graves, dependendo do caso. A IA, ao ser utilizada também em sistemas de grande escala (energia, transporte, etc.), pode gerar impactos significativos caso seja atacada.

- **Alucinações e direito à realidade:**

Os modelos de IA podem gerar respostas incorretas ou sem sentido, mesmo quando treinados da melhor forma possível, o que torna importante a conscientização sobre isso e a regulação da confiança nos algoritmos. Isso está relacionado a uma proposta interessante chamada *"Direito à Realidade"* que sugere que, diante de toda essa tecnologia, o ser humano tem o direito de acessar e conhecer a verdade. Assim, deve-se reduzir ao máximo as alucinações, fakenews, deepfakes e outras falsidades que uma IA pode produzir.

- **Preconceitos:**

As conclusões da IA podem perpetuar preconceitos presentes nos dados com os quais são treinadas, resultando em decisões discriminatórias em diversas áreas, como contratação de pessoal, questões legais, entre outras.

- **Desenvolvimento de ciberataques:**

A IA pode ser utilizada para desenvolver ou aperfeiçoar ataques cibernéticos, como, por exemplo, para análise ou geração de código malicioso.

DESAFIOS DE REGULAMENTAÇÃO

Diante do cenário que a implementação de IA nos apresenta, surgem várias questões legais que, na maioria das vezes, ainda ficam sem resposta.

- **Quem é competente para resolver questões sobre IA?**

A competência para resolver questões sobre IA é um tema complexo que ainda está em evolução, pois envolve várias disciplinas, não apenas o direito, mas também a tecnologia, a ética, entre outras. É difícil determinar em qual território seriam julgados os prejuízos causados pela IA, ou qual tribunal seria competente, por exemplo. Pode ser necessário estabelecer um acordo a nível internacional, visto que a implementação da IA transcende os limites geográficos.

Quem é responsável pela IA?

Se o uso da IA causar prejuízos, quem será o responsável por esses danos? Este é talvez um dos temas mais discutidos atualmente, já que há vários envolvidos a quem a responsabilidade poderia ser atribuída. Por um lado, temos os desenvolvedores da IA, que devem criar o modelo de forma segura, garantindo sua confiabilidade. Depois, temos as empresas que comercializam o modelo, que devem supervisionar o produto para minimizar seus riscos. E, por fim, temos o usuário final, que deve utilizar os modelos de forma responsável, cumprindo os termos e condições.

Dependendo do caso, a responsabilidade pode ser compartilhada. No entanto, como mencionamos, a legislação internacional ainda não resolveu essa questão.

A IA executa feitos ou atos?

Quando um ser humano causa um prejuízo, por exemplo, esse dano é o resultado de um ato realizado pela pessoa em questão. Esses atos são feitos realizados com discernimento, intenção e liberdade, e sua consequência, em primeira instância, recai sobre o responsável.

No entanto, ao pensar nas consequências causadas pela IA, sendo ela uma tecnologia sem capacidade de raciocínio e emocionalidade, podemos concluir que ela não realiza atos, mas apenas gera fatos. E, diante disso, voltamos à questão anterior: quem é responsável pelas consequências desses "feitos"?

AVANÇOS A NÍVEL REGULATÓRIO

- Com o objetivo de organizar tudo o que diz respeito à IA, alguns países têm trabalhado em regulamentações internas, e a nível internacional, tem havido pequenos avanços.

Podemos destacar:

- *Convênio Marco do Conselho da Europa sobre Inteligência Artificial e direitos humanos*, democracia e Estado de direito, que durante 2024 foi aberto para assinatura e pode ser considerado como o primeiro tratado internacional

vinculante (obrigatório). Entre os países que assinaram estão Andorra, Geórgia, Islândia, Noruega, República da Moldávia, San Marino, Reino Unido, assim como Israel, Estados Unidos da América e a União Europeia.

- Em 2021, pudemos ver as *Orientações da UNESCO*, que foram um marco ético, embora não vinculativo.

- Durante 2023, destacou-se a *Lei da União Europeia sobre IA* (possivelmente a norma mais completa atualmente, com um enfoque baseado na classificação da IA conforme os riscos), a Política Nacional de IA dos Estados Unidos e a ordem executiva do presidente Biden, e mais recentemente, o tratamento, por parte dos Estados Unidos, de um Projeto de Lei sobre IA (IA Blueprint).

- No Brasil, está em processo de aprovação um marco regulatório para a inteligência artificial. Em outros países da América Latina, os avanços durante 2024 foram limitados, com *exceção do Peru* que já conta com uma legislação específica sobre o tema

- O Parlatino (Parlamento Latino-Americano e Caribenho) criou, em 2017 *uma lei modelo para os países membros* com o objetivo de promover a regulamentação da inteligência artificial. Essa lei modelo propõe princípios éticos, bem como mecanismos de governança e proteção de dados.

- Podemos destacar que a regulamentação da IA de forma individual seria insuficiente, já que a questão também está atravessada pela normativa de proteção de dados e cibersegurança.

3

AS TECNOLOGIAS OPERACIONAIS (OTS) ESTÃO NA MIRA

Martina López
Security Researcher na
ESET América Latina

Historicamente, os sistemas industriais foram projetados para operar de forma analógica e isolada, mas depois começaram a incorporar tecnologias com um foco voltado para garantir a confiabilidade e a disponibilidade, mais do que a segurança. Essas implementações tecnológicas surgiram com a introdução de características da tecnologia da informação em sistemas físicos já existentes, com o objetivo de substituir mecanismos físicos secundários e introduzir novas funcionalidades, sem encurtar o ciclo de vida industrial do sistema, como ocorre nos sistemas 100% digitais.

No entanto, essa crescente integração e entrelaçamento com a digitalização, além do recente crescimento da Internet Industrial das Coisas (IIoT), expõe esses sistemas complexos a ameaças maliciosas, muitas vezes personalizadas e com diferentes motivações.

Os incidentes direcionados a Tecnologias Operacionais (OTs, pela sigla em inglês) têm se tornado cada vez mais frequentes, com ameaças que vão desde o famoso Stuxnet, passando pelo *NotPetya*, até o *Triton*. Esses incidentes mostraram que comprometer sistemas OT não afeta apenas organizações ou instituições, mas pode desencadear crises nacionais com impactos econômicos, sociais e até ambientais.

O QUE É A TECNOLOGIA OPERACIONAL?

A Tecnologia Operacional refere-se a uma categoria de sistemas e dispositivos programáveis projetados para interagir com ambientes físicos em contextos industriais. Esses sistemas têm como objetivo monitorar, controlar e gerenciar processos ou eventos que impactam diretamente os ambientes físicos. Exemplos comuns de OT incluem o controle de temperatura em um processo industrial, a regulação do fluxo de componentes químicos ou o monitoramento de cargas de outros sistemas dentro da infraestrutura de produção. Em resumo, OT engloba todas as tecnologias que permitem que as operações industriais sejam realizadas de maneira eficiente, segura e controlada.

OT abrange os sistemas que controlam e monitoram processos físicos em indústrias críticas, como energia, manufatura, transporte e abastecimento de água. Esses sistemas são o coração das infraestruturas que sustentam a vida moderna, desde a rede elétrica até as estações de tratamento de água e os sistemas de transporte público.

Entre os sistemas OT mais comuns, encontramos a Internet das Coisas Industrial (IIoT), os sistemas de Controle Supervisório e Aquisição de Dados (SCADA), os Controladores Lógicos Programáveis (PLC) e os Sistemas de Controle Distribuído (DCS). Juntos, esses sistemas formam, junto a controles manuais e operadores, uma topologia de rede complexa, cuja implementação envolve detalhes que estão além do escopo deste documento.

ADVERSÁRIOS DA TECNOLOGIA OPERACIONAL

No campo da Tecnologia Operacional, as consequências de um ciberataque não se limitam a perdas econômicas ou à exposição de informações confidenciais. Aqui, como em muitos casos, estamos lidando com infraestruturas críticas, e os ataques têm o potencial de causar interrupções significativas em serviços essenciais, como fornecimento de energia, transporte ou produção industrial, e até mesmo colocar em risco a segurança física de pessoas e infraestruturas.

Esses ataques transcendem o digital, tornando-se ameaças ao ambiente físico e, por fim, à estabilidade social e econômica. E é nesse ponto que se encontra o atrativo para os cibercriminosos, com motivações tão diversas quanto eles mesmos.

Na diretriz de cibersegurança para Tecnologia Operacional (OT) *publicada pelo NIST* são delineadas quatro categorias de agentes que representam riscos para a OT, dependendo da origem dos mesmos. Essas categorias são: ambientais (como catástrofes naturais), estruturais (falhas de hardware, software ou redes), acidentais (ações erradas tomadas por um indivíduo) ou adversariais.

Os agentes "adversários" são aqueles que classificamos como atacantes, em uma analogia com a abordagem de cibersegurança corporativa, mas com componentes adicionais. Eles são indivíduos, grupos ou estados que buscam prejudicar a empresa proprietária da infraestrutura, explorando sua dependência (adequada ou excessiva) de sistemas tecnológicos.

Devido ao seu grande impacto, este tipo de ciberataque é escolhido por atacantes cujas motivações se concentram na destruição ou alteração do funcionamento dos sistemas. Um caso muito lembrado foi o do *Industroyer*, um código malicioso modular projetado para afetar esse tipo de infraestrutura. Especificamente, essa ameaça utiliza quatro componentes maliciosos (payloads), que são criados para obter o controle direto de interruptores e disjuntores em uma subestação de distribuição de eletricidade por meio de protocolos de comunicação específicos de OT. Com esse controle, o código malicioso foi capaz de usar uma de suas funcionalidades: a negação de serviço, afetando uma planta de energia na Ucrânia.

No entanto, é essencial não negligenciar os cibercriminosos que buscam ganhos financeiros, seja como único objetivo ou como um entre vários. De fato, já fomos testemunhas desse tipo de ciberataque, especificamente aqueles que utilizam o ransomware como ameaça principal. Um exemplo amplamente conhecido foi o incidente com o Colonial Pipeline em 2021, um importante oleoduto de combustível nos Estados Unidos que teve sua operação interrompida por um ataque cibernético atribuído ao grupo DarkSide. Embora os detalhes do ocorrido não tenham sido completamente revelados, sabe-se que o atacante

usou uma conta comprometida de um serviço de VPN para lançar a ameaça e, em seguida, exigiu um resgate.

PLANEJAR ESTRATÉGIAS DE CIBERSEGURANÇA

A cibersegurança em tecnologias operacionais desperta preocupações tanto em órgãos governamentais quanto em setores privados. Surge, então, a necessidade (ou pelo menos o interesse) de incorporar uma estratégia de cibersegurança adequada ao risco de um possível incidente. De fato, as estratégias voltadas para a proteção da Tecnologia Operacional geralmente dedicam seções inteiras à avaliação e gerenciamento do risco: aqui não intervêm apenas perdas econômicas por inatividade ou consequências legais, mas também impactos no meio ambiente ou na população em geral.

As abordagens sugeridas por diversos especialistas em cibersegurança incluem uma proteção multinível, considerando todos os elementos envolvidos no ciclo de vida da Tecnologia Operacional: hardware, software, redes, acessos físicos e, é claro, os operadores. Nessa linha, agências de cibersegurança de diferentes países publicaram, em 2025, um *guia para responsáveis por Tecnologias Operacionais* com considerações de segurança ao escolher produtos tecnológicos para seus sistemas. Por fim, também existem equivalências aplicáveis de modelos de cibersegurança corporativa, como o Zero Trust, que podem ser considerados para sistemas industriais.

No entanto, apesar do grande desenvolvimento das indústrias que mais utilizam OT no Brasil e na América Latina, esse tipo de modelo ainda é um plano para o futuro. Seja por falta de interesse político, orçamento, simples desconhecimento ou uma sensação de distanciamento em relação a esses incidentes (diferente de outras regiões do mundo), ainda há um longo caminho até a implementação dessas medidas de segurança.

O fato é que esses ataques estão ocorrendo com cada vez mais frequência, e já podemos ser testemunhas de pelo menos um ataque de grande impacto por ano. E, embora com impacto variável e, em alguns casos, menor do que em outras partes do mundo, o Brasil e outros países da América Latina não estão imunes a isso: desde fornecedores de rede, passando por empresas de fornecimento de energia elétrica, até aquelas dedicadas à mineração.

O progresso nesse tema na América Latina não é insignificante. De fato, vários governos já o incorporaram em seus planos de desenvolvimento de cibersegurança para os próximos anos, sendo que, em novembro, o *governo chileno realizou uma simulação de ataque*.

Os próximos anos serão decisivos para avaliar se as medidas atuais são suficientes ou se enfrentaremos uma constante corrida entre a proteção e os ciberataques no âmbito da OT. O que é claro é que esse tema continuará sendo fundamental na agenda de cibersegurança global e regional, estabelecendo desafios que seguirão nos acompanhando no futuro.

CONCLUSÃO

Ao longo deste relatório, foram abordadas as tendências que podem marcar o ano de 2025, desde a inteligência artificial generativa e seus desafios, tanto no campo da cibersegurança quanto nas questões normativas e éticas, até os sistemas digitais usados para controlar processos industriais e físicos em diversos setores, os chamados Sistemas de Controle Industrial ou Tecnologias Operativas. É fundamental considerar cada uma dessas questões para este ano, pois as ameaças cibernéticas estão em constante evolução e buscam ativamente maneiras de contornar novas tecnologias ou controles de segurança.

Apesar de a Inteligência Artificial continua sendo uma tendência durante e pós-pandemia, como toda nova tecnologia, ela apresenta duas faces. Por um lado, seu impacto gerou novas capacidades defensivas, redefinindo a maneira como as organizações começam a pensar e agir frente aos aspectos de cibersegurança. Por outro, surgem várias questões, o que exige que os governos e instituições tenham a capacidade suficiente para responder a questionamentos como: com que qualidade de dados os modelos de Inteligência Artificial estão sendo treinados? Quem e como supervisionaram e selecionaram esses dados? Existem medidas que permitam aos algoritmos detectar vieses para garantir a imparcialidade na identificação e no enfrentamento de padrões discriminatórios nos dados? Que tipo de algoritmos são mais adequados para treinar esses sistemas? Sob quais critérios esses sistemas tomarão e poderão tomar decisões?

O que foi mencionado anteriormente pode deixar lacunas nas futuras legislações, as quais cibercriminosos poderiam explorar para adquirir e treinar seus próprios modelos de Inteligência Artificial, ou, no pior cenário, usar sistemas que não cumpram as normas para gerar códigos maliciosos mais sofisticados, além de ataques de engenharia social muito mais convincentes (como deepfakes e interações com realidade virtual).

O que aconteceria se a rede elétrica de uma cidade fosse comprometida por um ciberataque? A história já nos demonstrou que isso é possível. As consequências não se limitariam apenas ao impacto financeiro e tecnológico, mas também colocariam em risco a vida de centenas de pessoas.

Qualquer ativo no ciberespaço pode ser vulnerável, e é por isso que as organizações devem implementar políticas e controles de segurança que protejam o que, atualmente, é o bem mais valioso que possuem: a informação. Não podemos deixar de lado que a capacitação constante em cibersegurança para todos os níveis hierárquicos da organização é fundamental para reduzir consideravelmente os ciberataques. O elo mais suscetível dentro de um sistema digital, e onde a maioria dos ciberataques é bem-sucedida, é o usuário final.

A compreensão das ameaças previstas para 2025 pode ajudar as organizações a se anteciparem a possíveis agentes emergentes, fornecendo uma base sólida para definir ou atualizar as políticas de segurança em toda a sua estrutura. Adotar o modelo de confiança zero (Zero Trust) permitirá garantir a proteção do ambiente digital e fomentar um progresso contínuo.

Esperamos que este relatório ajude a compreender melhor uma parte do cenário que está por vir, promovendo assim a colaboração para fortalecer as defesas digitais, antecipar as ameaças emergentes e proteger o patrimônio digital em um ambiente cada vez mais complexo e sofisticado.

CYBERSECURITY
EXPERTS ON YOUR SIDE