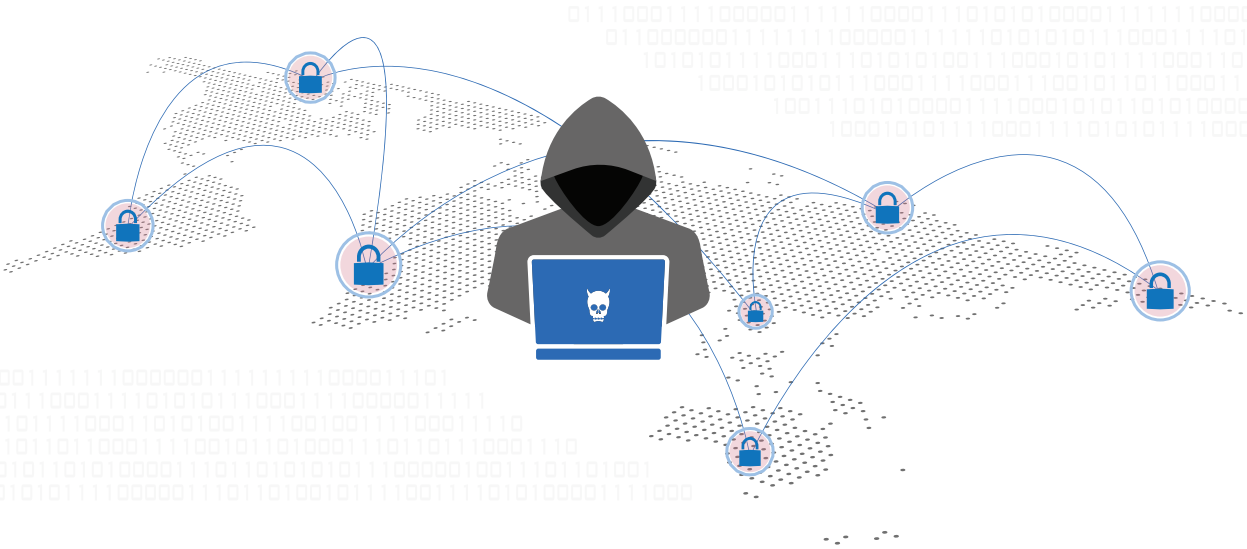
KELLTON TECH

WHITEPAPER

Artificial Intelligence and the Shifting Sands of **Cybersecurity**

Introduction

One of the biggest problems that besets today's internet age is cyberattacks. The last decade has witnessed hundreds of cases resulting in massive data breaches and loss of money. The future is rife with even greater dangers. As the complexity of systems and networks increases, cyberattacks, in parallel, are becoming more sophisticated and harder to detect. Any threat, irrespective of the type, can affect every person and organization alike. Given so, the need for building strong defenses to protect what's our own has never been more critical.



As digital businesses grow, their risks of cyberattacks multiply. A Juniper Research report noted that cyberattacks accounted for about $2 trillion in losses for the year 2019. Reflecting on the fragile state of the global economy, Cybersecurity Ventures, in another report, claimed that approximately $6 trillion is expected to be spent on the control of cybercrime by 2021. Growing concerns over safeguarding the proprietary information have forced the global enterprises to reassess the technology spends and invest where they can get the maximum bang from their buck. Interestingly, half of them have exuded confidence in Artificial Intelligence or AI and its revolutionary potential in minimizing cyberattacks—and averting future consequences.

This whitepaper tries to explore the power of AI in curbing cyberattacks and helping organizations achieve a renewed sense of resilience in the face of unprecedented odds. This document also pans its view to study the most promising AI use cases in cybersecurity and how each of these can facilitate new opportunities for value creation. Identifying threats to AI adoption can help leaders leverage their investments more beneficially. So, we have discussed a few challenging scenarios where AI can end up making cybercrime more powerful than it ever was instead of counteracting it.

The Current State of Global Cybersecurity

Cyberattacks and data breaches have exponentially grown in scale and severity over the past few years. Trillions of dollars have been siphoned so far, and there's no breather in sight. The WannaCry attack of May 2017 crippled the hospital facilities across the UK and triggered chaos elsewhere. A few months later, Petya ransomware wormed its way in, targeting Ukrainian government bodies and invading business systems across Europe and the US. In 2018, a virulent ransomware attack by Iranian hackers paralyzed operations at Atlanta's city hall for five days. British Airways Hack, Quora Breach, and Wipro Phishing Attack are an extension to the already long list of cyberattacks that rattled the world order.

Juniper Research, in a report titled "The Future of Cybercrime and Security: Threat Analysis, Impact Assessment, and Mitigation Strategies 2019-2024", claimed that the cost of data theft is expected to rise annually at 11%, from $3 trillion to $5 trillion per year. The report also observed that lack of awareness is the single biggest reason why enterprises are struggling to tame cyberattacks. Research author Susan Morrow advised that "All businesses need to be aware of the holistic nature of cybercrime and, in turn, act holistically in their migration attempts. As social engineering continues unabated, the use of human-centric security tactics needs to take hold in enterprise security." Notably, this is apropos of the fact that security awareness and training is a credible tool of fighting against the recent spurt in cybercrime and can help companies identify areas which need more attention.

World Economic Forum, in its annual report, pointed out that cybercrime is the biggest perceived threat in North America and Europe, and second globally. Over 12,900 executives from 133 countries participated in the survey, citing the five global risks that will become the greatest menaces for the business world in the next 10 years. "The fact that cyber threats worry the business community as much as they do academia, civil society, governments, and other thought leaders shows just how disruptive this risk is to all aspects of life," the report noted.

Cut to healthcare, the Food and Drug Administration sent shockwaves when it revealed potentially serious cybersecurity flaws in some medical devices. The regulator affirmed that medical devices using third-party and fairly obsolete software called IPnet were at risk, and the vulnerabilities could allow hackers to take control of devices and create logical flaws that could hamper their functioning. This spelled a chronic reality for the global healthcare industry. A hack of the 'said' nature could manipulate or steal patient data, hijack drug infusion devices along with several critical others such as pacemakers and insulin pumps, and paralyze the status-quo. The FDA started working with the subject matter experts and other stakeholders to understand the looming threat and identify medical devices at risk.

Speaking of the 2020 US presidential vote, we all recognize the phenomenal importance of the event and how it will redefine the international political trajectory. As the nation warms up for the exercise, reports suggest that the cyberattack cells have activated to influence the election outcomes. According to Microsoft, political parties, campaigns, and pro-democracy groups are under duress due to more than 800 cyberattacks in the past year. In a precautionary move, those who are involved in the democratic process have been asked to ensure basic cybersecurity hygiene.

While one might expect these attacks and insights would have helped enterprises identify the red flags, not much has changed. Several organizations overlook the need for cybersecurity investments and continue to rely on standard damage controls. Doing so, they merely turn blind to the kind of havoc that would ensue if a threat breaks in. And make no mistake about it: technological acceleration is a double-edged sword. Much as it brings certain advantages, its complexity and ubiquity is an opportunity for cyberattackers to exploit.

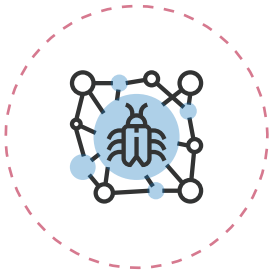
Emerging technologies like AI are playing a starring yet paradoxical role: They are a boon, but also a bane.

Artificial Intelligence in Cybersecurity: What's Changing and How?

As cyberattacks mature in technique, organizations are increasingly finding themselves exposed to several financial and reputational consequences. Last year, several high-value intellectual properties were entangled in an international web of espionage. And, given how cyberattackers are exploiting the third- and fourth-party supply chain partner environments to hack the target systems, it's apparent that basic measures, such as firewall implementation and backup management, offer limited help. Today's always-on, ever-connected business world needs intelligence and technological readiness as driving forces to win over cyberwarfare. Automated systems, using human-like ingenuity based on Artificial Intelligence, are the solution to this difficulty.

Artificial Intelligence or AI has emerged as a proactive force in curbing cyberattacks. Curating intelligence from data, the technology can help decision-makers with insights for automating event monitoring and incident response. Increasingly able firewalls, powered by Machine Learning (ML), can facilitate anomaly detection in web requests and automatically block those that carry a whiff of threat. Experts have also pinned hopes on the natural language capabilities of AI to lead cybersecurity innovation. The theory suggests that by scanning troves of data, AI systems can obtain a better understanding of how an attack occurred in the first place and suggest solutions to reverse the damage. Besides, the technology can play a part in addressing the skill shortage by empowering machines to sense, think, and act like humans and beefing up the existing cybersecurity capabilities with automation.

These possibilities suggest that AI has come past its days of boardroom resistance and been emerging as a go-to technology for business leaders to unlock cybersecurity value. But, these possibilities aren't all that AI can do. How this technology can stop the ticking time-bomb on cybercrime is a bigger story to tell. Here are a few ways Artificial Intelligence can control cybercrime and ramp up security on the web.

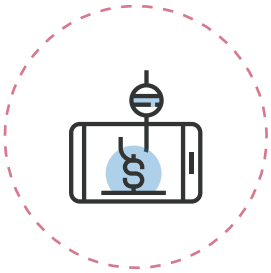


Preemptive Threat Detection

For years, global sustainability felt threatened in the face of evolving cybercrime. However, with AI on the frontlines, preemptive threat detection is evolving to become a new industry standard. The technology can empower systems with the ability to analyze data and identify patterns, which are suggestive of threats and can prompt organizations to forestall disruption. Given how the conventional technologies have succumbed to tame the cyberattacks, breakthroughs such as AI enable machines to have cognition and propose heightened control measures.

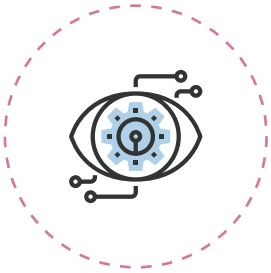
Password Protection and Authentication

Passwords are hackable, and biometric authentication doesn't make for a strong defense either. Lately, the proliferation of deepfakes has defined a new threat vector leading to widespread manipulation and hacking of biometric systems. Adding more to the quandary is the new crop of cybercriminals, who are skilled in the craft of hacking and know how to circumvent the security—both physical and logical. Given such precarious times, we must direct our attention to where the next threat to our collective security will come from and tip the scales using AI.



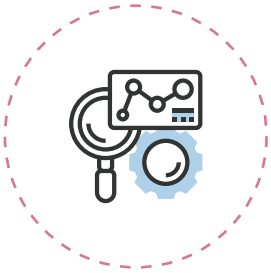
Phishing Detection and Prevention Control

The modern era of phishing is exemplified by emails by cybercriminals posing as genuine and pulling out all the stops to siphon data or money. Statistics suggest that over 92.4% of malware is delivered by email, thanks to the accessibility it provides. However, as AI makes inroads in the cybersecurity space, the problem might soon be solved. AI and ML show promise in tracking active phishing sources and remediating much faster than humans. Additionally, AI can scan phishing threats all over the world and filter out legitimate web sources from the fake ones effectively.



Vulnerability Management

Within this year alone, over 2,000 vulnerabilities have been reported with varying degrees of sophistication. At a time when cybercrime continues to rear its ugly head, advances in AI have shown promise to nip the threats in bud and augur well for the future. AI-based systems can proactively analyze real-time data to identify vulnerabilities that might hit home soon. Their ability to forecast events can help enterprises lay out preparatory measures much in advance and recruit resources necessary to disarm the threat.



Behavioral Analysis

ML algorithms can glean user insights to determine what the normal behavior of everyday users is, and raise the red flags when any malicious, stealth movement comes to attention. By zeroing in on these anomalies, security teams can execute their plan of defense early on and proactively stop the cyberattack. For instance, if an attacker tries to input a shipping address other than what the user usually recommends, ML algorithms can sound a security alarm and help those in-charge to take stock of the situation immediately.

Today's always-on, ever-connected business world needs intelligence and readiness to combat cyberwarfare. AI offers both.

The Lurking Dangers

AI, in the wrong hands, can act in ways inimical to the web security of millions. It's perceived that machines if develop sentience and intelligence of a human, will open the floodgates for more seamless and robust attacks that never existed in the first place. Below, we have discussed a couple of challenges that will strong-arm the whole human civilization if cybercriminals learn to exploit AI.

Attackers Weaponizing AI

With growing advances, AI is believed to not only supplement the defending but also the attacking side. AI-enabled phishing attacks have become a reality wherein hackers can bypass multiple layers of encryption and water down the data. Cybercriminals are turning to AI to counter the advancements in security solutions and launch intelligent malware attacks that self-propagate over a system or network while exploiting unmitigated vulnerabilities. The future may see AI empowering the bots to solve captcha with 89% accuracy and hence paralyzing the most essential tool used for differentiating humans from robots. Given such instances, there is no denying that a new phenomenon called 'AI attacking AI' is gradually emerging, sending global economies into a tizzy.

AI Breaking Away from the Human Control

While AI is found to be effective against cybersecurity risks, researchers said that if made too self-assured, the technology can override human orders. Once autonomous, AI can lead to a machine uprising that may wipe out the human race. It's worth noting that robots and other hyper-intelligent machines will never be able to simulate empathy and contextual capabilities as humans, and if strayed too far, they may wage cyberwarfare.

Data Tampering—A Slippery Slope

Data tampering can render AI powerless in terms of combating cybercrime. Attackers can rig algorithms with malware codes, sabotaging the integrity of data and tricking systems into believing false inferences. As a result, machines can fail to pursue correct decisions, and their ability to defend against cyberattacks can be severely impaired. It must be noted that once an anomaly is injected and not removed, it soon becomes an accepted part of the structure, which allows intruders to cloak their activities and hack into the target systems. Though AI is skilled in pattern recognition, it's unable to point out threats when it's trained on unqualified data.

A Breeding Ground for New Cyberattacks

Rapid advancements in AI are inspiring new types of cyberattacks and upsetting the already precarious apple cart. The technology is overstepping the human potential of hacking into a system's vulnerability in terms of speed and method. The time is ahead when AI can be used to disguise attacks in a way that a breach would go unnoticed for days. Cybercriminals will soon learn to employ quantum computing and blend it with AI to concoct attacks of an unprecedented nature.

Though the challenges are undisputed, the good can still outweigh the bad if the human element continues to steer the transformation of cybersecurity in the age of AI. Autonomy should be sparse, and 'balanced intervention' should remain the operative word. While AI is imperative to redefine the status-quo of cybersecurity, it's equally essential to ensure that the technology doesn't spiral out of the human control and go on a rampage.

About the Author

Sushil Kumar Tripathi is working as Vice President - Technology at Kellton Tech Solutions Ltd. He has worked on multiple technologies which include and are not limited to AI/ML, Analytics, AR/VR, Drupal, LAMP, Java/J2EE, .NET, Node.js, and more. Sushil is an expert in system design and has worked as a Solution & Technical Architect for years across all major technologies in web and mobile and IoT space.