AI and Cyber Resilience

A race between attackers and defenders

www.link11.com

AI and Cyber Resilience: A race between attackers and defenders

The development of artificial intelligence (AI) is galvanizing the economy, society and politics alike. In philosophical debates, people are still questioning whether the benefits of AI for humans outweigh the risks involved in its use. Undeterred by this, various AI applications such as machine learning and pattern recognition and prediction are increasingly making their way into everyday life.

Insurance companies, meanwhile, are using AI systems to detect fraud and to handle cases. Banks and credit card companies also use such systems to detect fraudulent behavior, anomalies in use, and for other risk-prevention purposes. AI assists retailers with supply management or analysis of customer flows and sales figures. In medicine, AI supports imaging diagnostics and the analysis of large volumes of data, such as those generated during the fight against the Covid-19 pandemic.

Companies should not only deal with AI because their competitors are doing so and are energetically kick-starting a technological revolution. The active employment and utilization of AI is now particularly important in the area of cyber resilience and IT security. AI is regarded as a key technology for marshalling security measures to prevent cyber-attacks and boosting the resilience of a company's IT infrastructure. However, on the flip side, criminals have also discovered the benefits of AI.

Artificial intelligence: Artificial intelligence (AI) simulates human intelligence with machines, especially computer systems. This includes learning (the collection of information, rules and patterns for use), inference (the use of this learning to draw approximate or final conclusions) and self-correction. Special applications of AI include expert systems, speech recognition and machine vision.

Machine Learning: Machine Learning is the science of enabling computers to recognize patterns in existing data sets, and use them to improve their learning over time to find independent solutions to problems. It is therefore an important branch of artificial intelligence.

Deep Learning: Deep learning is part of the thematic area of machine learning. Algorithms inspired by the human brain (Artificial neural networks) learn from large amounts of data. Just like the Artificial neural networks, the process behind these algorithms is very similar to the human learning process from experiences. The deep learning algorithm performs a task repeatedly and makes small changes to continuously improve the outcome.

How criminals use AI

If your company's IT has not yet suffered a large-scale attack by criminals, you've simply been lucky. A common saying among experts is that there are only two types of companies: those that have experienced a major hacker attack, and those that don't know they've been attacked.

Criminals and hackers follow the development of AI as closely as companies. And like their corporate targets, the bad actors are taking advantage of this technology. Companies shouldn't delude themselves into thinking that AI is too complex or too expensive for criminals. Cloud providers such as Google, Amazon, and Microsoft already offer interfaces to machine learning computing systems. But it should not be forgotten that competitors, intelligence services, or states could also be launching online attacks. In such cases, money is irrelevant.

There are a number of ways that criminals take advantage of AI, including:

- **Biometrics:** Numerous impressive examples illustrate that AI can be used to digitally create deceptively real-looking people and faces. The systems can also use everyday images of the people concerned to create these so-called “deep fakes”. This makes it possible to circumvent biometric security systems that use face recognition.
- **Speech recognition and speech synthesis:** Applications that can artificially generate speech are similarly sophisticated. Google, for instance, has developed a voice synthesizer app that can handle appointments by phone. The callers don’t even notice that they’re talking to a computer system. By means of Natural Language Generation, attackers can imitate the voice and tone of voice of a trustworthy person and thus gain access to potentially sensitive information. Conversely, speech recognition and speech analysis can be used to obtain data from telephone recordings or other sources that can reveal details about security systems or provide information about upcoming transactions, which are then intercepted.
- **Machine learning:** Attackers employ machine learning to analyze the behavior of their victims using large volumes of company data. The aim is to develop promising phishing attacks. Machine learning can also be used to analyze weaknesses in security systems. Machine learning allows malware to be programmed in ways that can hardly be traced, or only to a very limited extent. An attack might use “self-learning” Trojans, for example.
- **(Predictive) analytics:** AI systems are commonly used to make predictions. Based on data already obtained from successful and repulsed attacks, intelligent systems can help the attacker develop a strategy for a promising attack. An AI system can also automatically identify vulnerabilities in IT systems.

Because of the amazing technical wizardry that AI makes possible – and the resulting threats cybercriminals can direct at digital business processes – companies should not hesitate to use AI to counteract such threats.

Cyber resilience is becoming increasingly important

In an increasingly digitalized business world, cyber-attacks often lead directly to business interruptions. According to the German industry association Bitkom, cyber-attacks inflict damage on the German economy to the tune of 100 billion euros every year.[1] Globally, cybercrime damages are predicted to reach $6 trillion annually by 2021, according to Cybersecurity Ventures.[2] Strengthening the resilience of IT infrastructure is therefore becoming an increasingly important corporate priority. To this end, vendors are developing new approaches and defining measures to ensure the continuation and resumption of business activities during or after a cyber-attack. For organizations, cyber-resilience means being well prepared to react promptly to security breaches and to counter security incidents while keeping business operations up and running.

Resilience to external attacks depends on the organization’s security culture and the protection solutions it uses. Both require a broad understanding of and buy-in to the implemented security concepts and control solutions. Given the highly dynamic security risk environment, a static approach – in which processes and protection solutions are defined once – is no longer sufficient. Organizations that invest strategically in new technologies can exponentially increase their cyber-resilience. According to the results of Accenture’s 2019 State of Cyber Resilience Report, companies that scaled their investments the most intelligently improved their cyber-resilience four times as much as others.[3] Evidently, AI and machine learning are the technologies of the future.

[1] Born2Invest: Why cybercrime is causing record losses for German companies, November 2019

[2] Cybercrime Magazin: Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021, December 2018

[3] Accenture: Third Annual State of Cyber Resilience, January 2020

CYBER RESILIENCE BENCHMARKS 2020

Innovation investment in cyber resilience is growing.

86%

the percentage of organizations spending more than 20% of their cybersecurity budgets on advanced technologies

US$ 380,000

average cost per attack for non-leaders

US$ 107,000

average cost per attack for cybersecurity leaders

72%

High-performance cybersecurity can help to **reduce the cost per attack by 72%**, amounts to US$ 273,000

Advanced and turbo-charging technologies which bring benefits to cyber security and cyber resilience:

- Artificial Intelligence and machine learning
- SOAR (Security, Orchestration, Automation, Response)
- Next Generation Firewall

How cybersecurity leaders using advanced technologies are doing things differently

- **4x** better at stopping attacks
- **4x** better at finding breaches faster
- **3x** better at fixing breaches faster
- **2x** better at reducing breach impact

Lessons to master cybersecurity execution

- Invest for operational speed
- Drive value from new investment
- Sustain what you have

Source: Accenture:
Third Annual State of Cyber Resilience, January 2020

http://www.accenture.com

AI is the clear leader when it comes to defending against attacks

AI is a neutral technology that is neither good nor evil at its core. In the hands of criminals, it poses a serious threat. But it can also be used for good and to ward off and reduce risks. Any attempt by humans to combat AI that threatens them is doomed to fail. The human brain alone is no match for AI. When it comes to IT, security solutions will benefit significantly from AI components, since they allow numerous weaknesses inherent to traditional solutions to be overcome.

1. AI is faster

As the digitalization trend evolves and grows, companies will be further challenged by the need to monitor and protect a growing number of applications, external cloud providers, and devices. In coming years, the number of systems to be monitored will explode due to the Internet of Things (IoT). Intelligent sensors in IoT devices can control domestic appliances, transmit information across the supply chain, or open the door to new business models. For instance, a billing model based on the actual use of devices (i.e., pay per use) is inconceivable without sensors.

Conversely, this means that the volume of data processed by an organization will continue to grow and the number of interfaces and communication channels within the company will increase. However, it's a well-known fact that every additional channel embedded in the IT landscape is a potential gateway for attackers and criminals. Automated AI systems that monitor the data traffic of IoT sensors, for example, can detect anomalies in their behavior much faster. They can sound the alarm or initiate countermeasures faster than humans ever could.

The headlines over the past 18 months have made it increasingly clear that encryption Trojans and ransomware pose major threats to the public and private sector. We are referring here to the failure of entire computer network systems in hospitals. As a survey by Sophos revealed, the average cost to an organization of a ransomware attack (considering downtime, people time, device cost, network costs, etc.) is US $732,520.[4] Contamination by computer malware often happens through legitimate user accounts.

In large and possibly globally active companies, employees log on to internal systems around the clock – evidently, too often for many to check manually. In this context, AI can, for example, recognize peculiarities in order to respond appropriately on the basis of predictive analytics and pattern recognition. If an employee usually logs on to a company system from a defined region during fixed working hours, a successful logon in the middle of the night, from a different time zone or a completely different region is at least suspicious. Detecting such an incident manually is like looking for a needle in a haystack.

2. AI never misses anything

Large-scale attacks take some preparation and time to get started. During this time, the attackers try to get as many systems or attack vectors as possible into position. In doing so, they often leave traces on hijacked systems. Using pattern recognition and analyses, AI-based defense systems can detect even minor deviations. Administrators and CSOs receive an alarm in time if the system classifies an incident as potential preparation for an attack.

In the event of an imminent DDoS attack, prompt action is required. But what still constitute normal organic growth in network traffic? And when is an increase in traffic indicative of an attack? AI brings its speed to bear in this context as well. Regular analyses of growth, data sources and characteristics of a DDoS attack are carried out within seconds. Here, the software is superior even to experienced employees, as it processes and analyzes multiple data sources, and can take countermeasures faster.

Conventional detection systems[1]	Detection systems with learning / AI component
Software (SW) works within rigid models	SW works with adaptive models
SW generates decisions based on a transparent rule system	SW generates decisions based on gradual evaluation
SW is not capable of learning	SW learns continuously
SW uses signatures and correlations against different types of data	SW learns complex patterns from a large amount of data
Updating of the SW is done by controlled update	SW is independently updating

[1] J. Müller-Quade: Künstliche Intelligenz und IT-Sicherheit. Bestandsaufnahme und Lösungsansätze, April 2019

3. AI is better than any patch

Repelling criminal attacks is often reminiscent of a game of cat-and-mouse. Typically, security solutions distinguish between "good" and "bad" requests or program code. If new security vulnerabilities are discovered, the reaction usually consists of manual adjustments. A patch is applied, the firewall parameters are changed and signatures of malicious programs are updated.

This is how the security systems are kept up to date. However, developing patches, updates and parameters takes time and applies to incidents that have already happened or security vulnerabilities that have already been discovered. Meanwhile, the criminals haven't been idle. They use other networks for attacks that are not yet covered by the firewall, exploit new security vulnerabilities or use so-called polymorphic malware, whose code constantly changes, making it harder for detection programs to do their job, while at the same time improving the malware's "disguise".

Analysis systems based on AI level the playing field against attackers. Self-learning AI systems, which constantly improve during use and thus automatically make their own decisions, are a powerful tool. In a "whitelisting" strategy, all network traffic is initially classified as harmful until the opposite is proven (that is, when all packet contents are analyzed). AI speeds up the analyses and decides which data streams are allowed to pass.

4. AI overcomes staff shortages

Across all industries, three parallel developments in IT security have emerged in recent years, the combination of which are cause for concern.

First, the number of attacks against companies has risen. The risk of phishing, successful attacks with ransomware, and DDoS attacks has intensified. As noted above, this is also due to the growing number of potential gateways and platforms. At the same time, new legislation has been passed which directly impacts IT security. In essence, the GDPR describes very precisely which "technical and organizational" measures companies and authorities must take to protect data from unauthorized access, manipulation, and theft. Consequently, IT security requirements are also increasing, and more specialist staff are required to implement compliance and respond to increased threats. The demand for IT security experts is exploding. However, many companies, especially small and medium-sized ones, do not or cannot manage to recruit these specialists at all. Global IT security skills shortages have now surpassed four million, according to (ISC)2.[5]

[4] Sophos: The State of Ransomware 2020, May 2020

[5] (ISC)^2: Cybersecurity Workforce Study.Strategies for Building and Growing Strong Cybersecurity Teams, November 2019

As expected, this has consequences: Existing staff are overworked and can therefore only devote themselves to important issues to a limited extent. It's no surprise that many organizations are still using outdated software and operating systems, which is exactly what makes companies more vulnerable to attack.

One significant economic factor is the so-called innovation backlog. Companies are very open to IoT solutions, but do not roll out projects because they fear security vulnerabilities and are worried about data protection.[6] The lack of skilled staff and fear of risks therefore impede technical innovation.

Using AI in IT security solutions saves human resources because machines can make many decisions independently (based on rules), analyze data faster, and can process considerably more data than humans. Unlike humans, AI systems do not get tired. Algorithms do not overlook anomalies when analyzing log files, while humans may already be tired or distracted because, for example, they want to go home for the day. AI therefore eliminates the human error factor.

In the future, companies will not be able to avoid using AI in IT security if they want to overcome the shortage of skilled workers and protect themselves against highly specialized criminals. According to a global survey by Forrester Research, 40% of corporate IT security decision makers are planning to implement AI.[7] There is a growing awareness among security leaders of the security potential of AI-based solutions. This has been confirmed by a survey by Capgemini.[8] Almost two-thirds (62%) of companies believe they will be virtually helpless against cyber-attacks without AI technologies to protect them. AI supports security experts in their day-to-day work and helps them focus on particularly urgent and time-critical tasks without having to compromise on overall security matters. The Capgemini survey provides concrete figures on how improves the level of protection for companies. Three out of four respondents (74%) reported faster responses to attacks, while 69% noted better attack detection. Sixty percent of respondents cited increased efficiency in cyber security analysis as one of the benefits of using AI.

There is strong and clear case for using AI in cyber security.

[6] Helpnetsecurity.com: Security remains a major concern for enterprise IoT integration, June 2020
[7] Forrester Research: Forrester Analytics Global Business Technographics Security Survey 2019
[8] Capgemini: Reinventing Cybersecurity with Artificial Intelligence, July 2019

MASTERING
CYBERSECURITY WITH AI

69%
of organizations acknowledge that they will **be not able to identify critical threats without AI**

Nearly
1 in 5
organizations
used **AI** in cybersecurity pre-2019

Almost
2 in 3
63%
organizations

PLAN TO **EMPLOY AI** BY 2020

28% are using security products with **AI EMBEDDED**

73% OF ORGANIZATIONS
said they were testing use cases for AI for cybersecurity in some way

Source: Capgemini Research Institute: Reinventing Cybersecurity with Artifical Intelligence, July 2019

How Link11 protects you better with AI

Link11 has addressed the question of how to improve AI security solutions and make companies even more resilient to cyber-attacks at an early stage. Machine learning, pattern recognition, and predictive analytics are becoming an integral part of a growing number of its services.

BOT-Management: Like AI, bots are not good or evil in themselves. The requests generated by these automated programs now account for a large portion of the traffic in many companies. Search engines use bots to index page content. Comparison portals use bots to obtain current price information. However, bots can also be used fraudulently and criminally – for example, when they fraudulently retrieve advertising formats or use criminal bots to restrict the usability of a system. Link11's BOT Management Service allows you to classify and control the traffic caused by bots on your systems. AI helps the system recognize and evaluate previously unknown bots. When using the service, artificial intelligence helps you to provide genuine users visiting your pages with a better experience by responding to the traffic generated by undesirable bots.

DDoS Protection: DDoS attacks are becoming increasingly common and complex. The Link11 DDoS protection solution uses the cloud in combination with artificial intelligence. Thanks to the cloud, the protection is highly scalable and can be deployed quickly. And its "Always On" feature means the system operates around the clock in the event of an attack, when time is of the essence. The AI solution learns in real time from all attacks repulsed by Link11. The system analyzes each attack and applies the results to other threat patterns. Unlike any manual approach, the system is therefore prepared for new attack vectors. This benefits all customers and companies, as the defense shield is constantly improving. It anticipates similar incidents and can therefore react faster and faster in case of danger.

AI systems are no substitute for personal responsibility

Despite its unmatched potential, artificial intelligence is not a panacea for IT security and cyber-resilience – at least, not yet. After intensive training, AI can indeed effectively detect threats such as malware or DDoS attacks. It's also more accurate than attack detection conducted by humans. However, as the threat situation in the digital world is highly dynamic, it will continue to be the job of humans to classify the attacks and derive measures from them. Artificial intelligence will be the most important means of support. It will increasingly relieve people of the decision-making burden, but will not replace them completely.

To learn more about how artificial intelligence can improve your IT security and help you implement your cyber-resilience strategy, contact one of our specialists today.

About Link11

Link11 is the leading European IT security provider in the field of cyber-resilience. The global protection solutions of the Cloud Security Platform are fully automated, react in real-time and defend against all attacks, including unknown and new patterns, in under 10 seconds. According to unanimous analyst opinion (Gartner, Frost & Sullivan) Link11 offers the fastest mitigation (TTM) available on the market. To ensure cyber-resilience, web and infrastructure DDoS protection, BOT-Management, API protection, secure DNS, zero touch WAF, secure CDN, and threat intelligence services, among others, ensure holistic and cross-platform hardening of corporate networks and critical applications. International customers can thus concentrate on their business and digital growth. Since the company was founded in 2005, Link11 has received multiple awards for its innovative solutions.

Link11 GmbH
Lindleystraße 12
60314 Frankfurt
Germany
✉ info@link11.com

Frankfurt Office
☎ +49 (0)69 – 264929777

UK & Ireland Office
☎ +44 (0)203 - 8688711
✉ info.uk@link11.com

Nordics & Baltics Office
☎ +46 (0)85 - 250 05 71
✉ info.nordics@link11.com

BeNeLux Office
☎ +31 (0)68 - 992 3607
✉ info.benelux@link11.com