

⟨o⟩ Muninn

We
See.
We
Act.

**CYBER
TRENDS** 24

Stepping Into the Future

CONTENTS

1_ Stepping Into the Future

3_ 2023 in Retrospect:

A Look at Cyberthreats across Industries

9_ The Long-Awaited

Upgrade: *NIS2 and what it means for cybersecurity*

13_ A New Risk Profile:

The Critical Challenge of AI Security

17_ Tomorrow's Lock

and Key: *Evolving Security Standards for the Post-Quantum Cryptography Era*

21_ From an AI Revolution to AI's Evolution:

What's to come in 2024

29_ Beyond the Hoodies:

Decoding the Realism of Hacking in Hollywood.

33_ The Next Generation of Cybersecurity

Dear reader,


There is one undeniable truth: change is inevitable, and recent years have shaken countries and societies globally. In 2023, Artificial Intelligence, notably Generative AI like large language models such as ChatGPT, took center stage as a transformative technology, reshaping various industries, including cybersecurity. How has it influenced the general perception of AI and bolstered cybercrime? What impact will it have once the hype is over? I am certain another high-speed race with ML-based adversarial awaits us in 2024, not just in terms of technological milestones, but also as we will witness the implementation of the first AI regulations and legislations.

However, the past year was a reality check for numerous organizations that fell victim to ransomware and other cyberattacks. In Denmark alone, several companies made headlines due to massive data breaches. In instances like CloudNordic and AzeroNordic, hackers disrupted company operations, resulting in the loss of access to customer data. While it may be too late for affected organizations, analyzing these attacks can better equip us against future cyberthreats.

In the coming years, we anticipate supercomputers to revolutionize cybersecurity with their exceptional decryption capabilities, and new post-quantum cryptography to take stage. Preventing unlimited access to all available encrypted data is an increasing area of focus.

Whether depicting AI dominating the world a decade from now or political hacktivism, observing how pop culture interprets the present and future can be a refreshing escape. For various and more entertaining reasons, Hollywood has tried to predict and portray cybersecurity for decades, sometimes more realistically than others.

Looking ahead to 2024, Muninn will continue in developing the next generation of Network Detection and Response (NDR) platforms. To address the gap when an attacker infiltrates your network, strong machine learning algorithms and a platform capable of handling and analyzing complex contextual information are essential. Amid constant change, in the future NDR might evolve into a tool not only showing current network activity but also predicting an attacker's next move.

A portrait of a middle-aged man with short brown hair, wearing black-rimmed glasses, a dark blue button-down shirt, and a dark blue blazer. He is sitting with his hands clasped in front of him, looking directly at the camera with a slight smile. The background is a plain, light-colored wall. A white metal railing is visible in the bottom left foreground, slightly out of focus.

Andreas Wehowsky

Andreas F. Wehowsky

A silhouette of a person with a unicorn head is centered against a solid green background. The person's hand is raised to their forehead in a thoughtful or distressed pose. The text is overlaid on the silhouette.

A LOOK AT CYBERTHREATS ACROSS INDUSTRIES

2023

IN RETROSPECT

2023 was a busy year in cybersecurity and by reflecting on the cyberattacks that happened last year, we can gain invaluable insights into potential patterns and trends that might become the new blueprint of cyberthreats in the upcoming years. With high-profile and state sponsored ransomware attacks dominating headlines this year, we want to take a look at how it affected different industries.

The rapid advancement of technology and generative AI has empowered the business as well as cybercriminals, which has become a major concern for organizations worldwide. The result is in an escalating number of security breaches with certain industry sectors being inherently more susceptible to cyberattacks than others.

[As of 2023](#), the global average cost incurred per data breach amounted to 4.45 million U.S. dollars, witnessing a surge from 4.35 million U.S. dollars in 2022 and thereby continuing the trend of previous years. Notably, the healthcare industry bore the highest average cost of a data breach. Understanding these potential threats becomes imperative for organizations, given the staggering impact of cybercrime on the global economy. [According to Statista](#), by 2026, annual cybercrime expenses worldwide could surpass \$20 trillion, indicating a mammoth 150 percent increase from what we are seeing today.

But the highest price to pay for any company is bankruptcy. After nearly twenty years of operation, the Danish cloud host provider, CloudNordic, closed this year due to a devastating ransomware attack in August 2023 that erased its systems and destroyed all its customers' data. Despite lacking the funds and refusing the idea of paying the hackers, the company, left with no alternative, ultimately shut down.

With such tragedies happening, businesses must invest resources in the handling of growing customer

data and robust cybersecurity measures to keep these sensitive data secure. Despite a marginal increase in the frequency of attacks, attackers have also orchestrated sophisticated campaigns by weaponizing legitimate tools for criminal purposes. Recent instances include leveraging AI models like ChatGPT for code generation, Trojanizing software like the 3CXDesktop app for supply chain attacks and exploiting critical vulnerabilities such as the unauthorized RCE Vulnerability in the "Microsoft Message Queuing" service (MSMQ).

Complacency is not an option and Chief Information Security Officers (CISOs) must prioritize the development and execution of a security strategy that eradicates blind spots and vulnerabilities across their entire digital infrastructure. This includes mitigating risks arising from shadow IT development environments, remote access vulnerabilities, or potential email vectors that could be exploited for breaches.

[Statistics from the first quarter of 2023](#) reveal a 7% surge in global average weekly attacks compared to the corresponding period in the previous year, with each organization facing an average of 1,248 attacks per week.

During this period, the Education and Research sector endured the highest number of attacks, averaging 2,507 attacks per organization per week—a 15% increase from Q1 2022. Meanwhile, the Government, Military and Healthcare sectors encountered 1,725 and 1,684 attacks per week, respectively, showing a persistent cyberthreat trend for these vital government sectors.

Despite ongoing challenges, institutions within the Education and Research sector continue to grapple with securing extended networks and access points, especially during the transition to remote learning—an issue that continues to weigh heavily on the sector's cybersecurity posture ■

HEALTHCARE AT RISK

Ransomware and Mistakes Threaten Data Security

By now this sounds like a tale as old as times, hackers are specifically targeting hospitals and medical facilities, causing chaos by locking down their systems with ransomware. This not only disrupts their ability to provide critical care but also puts sensitive patient data at risk. Although the number of attacks on hospitals hit its peak in 2021, the past three years have seen a rise in data breaches caused by ransomware. These breaches involve stolen data, making the situation even more dire for organizations struggling to keep their systems running.

When these attacks happen, it's not just about fixing the systems; it's also about dealing with the fallout. Medical staff have to keep working without their usual tools, causing disruption in patient care. Fixing these issues without reliable backups take a lot of time and resources, in a sector which is already lacking resources to begin with.

In addition to ransomware attacks, there's also a common human error called "Misdelivery." This happens when sensitive information meant for one person ends up in the hands of someone else entirely. Picture a scenario where a private health record meant for a specific patient gets sent to the wrong recipient. It could be a wrongly spelled email address or even a physical mail error where too much personal information is visible through an envelope's window. Whether it's accidental data leaks or information sent to the wrong hands, these errors are causing serious problems.

Now, employees can also pose a threat. While they might not be among the top three issues anymore, their misuse of privileges and snooping around out of curiosity are still causing security threats. Sometimes, multiple employees team up to cause breaches, which can be a real headache for the health care industry. In order to prevent these situations, healthcare organizations need to pay close attention to potential threats and unusual data access patterns to keep their systems and patients' information safe and secure.



CASE

Hacker Group Anonymous Sudan

In February 2023, the hacker group Anonymous Sudan targeted nine Danish hospital websites, causing them to go offline. Prior to this, the group had launched similar attacks on Danish airports and in Sweden. As a result of this attack, website services in the Capital Region of Copenhagen experienced a four-hour outage.

Despite its name, Anonymous Sudan is not affiliated with the long-standing group known as Anonymous. Their primary method involves DDoS attacks, which floods an organization's website or web infrastructure with an overwhelming volume of malicious traffic. This traffic can cause a website to shut down, preventing legitimate users from accessing it.

While the group later claimed their attacks were a response to Quran burnings in Denmark and Sweden, reports from cybersecurity firm TrueSec suggest strong connections to the Russian government. During Q2 of 2023, the group collaborated with the pro-Russian hacker group Killnet on further attacks.

In contrast to many other attack groups, research indicates that Anonymous Sudan does not use a botnet of infected personal and IoT devices for their assaults. Instead, they have employed a cluster of rented servers—capable of generating higher traffic than personal devices—to execute their attacks. The financial capacity to rent these servers raises doubts among some researchers, who question whether the group truly represents the grassroots hackers they claim to be.

CYBERTHREATS IN FINANCE

Big Money, Big Risks

The financial industry is like a jackpot for cybercriminals. Banks don't just have a lot of cash but also handle and have access to sensitive customer information. Cybercriminals have a variety of tricks to mess with banks and other financial institutions, like phishing, ransomware, and sneaky social engineering scams.

And as everything related to money becomes more and more digital, it's opened up new ways for these hackers. Mobile banking, digital payments—are all new attack surfaces and increase the risk for trouble. From malware for mobile devices, hijacking online accounts and fake transactions, the list of possibilities is long.

Cybersecurity within the financial sector needs to be as serious as some of their representatives look like: multi-factor authentication, regular software and security updates as well as frequent employee training are essential and standard.

But why work hard when very little effort sometimes brings you far? One would be surprised how many times hackers just brute-force their way into a network or use password they acquired from other data breaches. These simple attacks are actually pretty successful for the bad guys. The not so complex Basic Web Application Attacks pattern seems to be working fine for cybercriminals, since they are what is seen most in this industry.

Other attack patterns involve Misdelivery, where data gets sent to the wrong person—whether this is a letter or an email flying off to the wrong inbox.

Interestingly, ransomware isn't as hot a choice for finance these days and System Intrusion has dropped [from 27% to 14% in 2023](#). Maybe because hackers have to roll up their sleeves and really work for it, while other more simple attacks seem to have a higher cost to benefit ratio. Regardless ransomware attacks remain a headache.

CASE

Security Vulnerabilities MOVEit

A data breach revealed at the beginning of July 2023 at several financial services providers turned out to be larger than previously thought. Besides Deutsche Bank and Postbank, which had already acknowledged unauthorized access to sensitive customer data, additional financial institutions were affected as well: both ING and Comdirect, which belongs to Commerzbank, collaborated with the service provider Kontowechsel24.de.

The company Majorel, which includes Kontowechsel24.de, cited a security vulnerability in their software MOVEit as the cause of the data breach. While the exact number of affected customers couldn't be specified, it was stated that the data stolen consisted of customer names and international bank accounts information.

It remains unclear who was responsible for the data breach.



PRODUCTION LINE

The Manufacturing Maze

As production gets more technology heavy and connected, they become highly interesting targets for cyberattacks. Manufacturing companies face all sorts of dangers—like supply chain hits, espionage of intellectual property, and the classic - ransomware attacks. However about 67% of incidents in this sector are Denial of Service attacks and it's been on the rise for a while.

Hackers can hold whole supply changes hostage by sneaking into their systems or are able to steal intellectual property, to use it for their own gains or simply re-selling it.

Ransomware attacks are on the rise, as they can be disruptive to whole production lines, and even hit the supply chains. This headache can cost these companies huge revenues and moreover their good reputation.

Cybercriminals know the importance of manufacturing and our daily life depends on certain supply chains. They see a huge opportunity to make money by exploiting this sector. Therefore, financially motivated external actors are still the biggest issue for this industry.

To sum it up: When we zoom in on the Manufacturing world, it's clear hacking and malware are the big players. Social attacks are in the game, too. Ransomware, which causes a lot of chaos in system breaches, keeps slowly creeping up in this industry.



CASE

The Aftermath of Ransomware

In October 2023, Röhr+ Stolberg, Germany's leading manufacturer of lead sheet and lead wool, fell victim to a ransomware attack, as stated by the company. The incident caused significant disruptions in their operations and made communication with customers and suppliers more challenging as all servers had to be shut down.

The company communicated on October 30, 2023, that all servers were successfully restarted after a week, ensuring communication through secure channels such as phone and other devices that were not connected to the affected network parts.

Röhr+ Stolberg did not rule out the possibility that cybercriminals may have stolen the company's data. However, the incident and its aftermath caused a severe disruption in their business flow.

ON HIGH ALERT Battleground Government, Public and Educational Sectors

The government is a real treasure chest for all kinds of sensitive information. So, it's no surprise that in this sector espionage driven attacks are consistently among the highest. Whether it is external, internal or both actors working together to steal data and attacks are often carried out by nation-states or state-sponsored groups.

Insider threats whether intentional or accidental, such as a government employee accidentally emailing sensitive information to the wrong recipient, are also a big concern for the public sector. Don't underestimate the role of social engineering attacks, such as phishing or spear-phishing attacks, as government employees face a significant amount of these attacks as well.

What's even worse? Sometimes, these hackers might team up with unhappy insiders. The good news is that these internal threat actors peaked in 2019 and have decreased slightly since then. But catching these espionage insiders early can save a lot of trouble.

Ransomware being used for the System Intrusion pattern remains one of the top methods for cybercriminals to be disruptive and make money. However, the data suggest that it might be less favored, due to its slight decrease.

When looking at the educational sector, there's been a shift in the top three patterns. The usual mess-ups—like sending information to the wrong place and other errors—have slightly increased. Social engineering increased [from 14% \(2022\) to 21% \(2023\)](#), especially phishing, which showed up in 18% of breaches. Hacking and malware are big players, shown in [80% of all breaches](#), with ransomware making up for nearly a third of all breaches in this sector.

What stays the same for the educational sector is that financially motivated external as well as spying nation-states are the most interested threat actors and personal data remains the most often stolen data type.

CASE

Cyberattack on Schools in South Denmark

In August 2023, students and staff at five schools in South Denmark have had sensitive personal information leaked following an extensive hacking attack by the group Rhysida. The attack occurred after a student connected an infected computer to the school network on August 27th.

The incident was discovered on August 31st, when hackers had encrypted the network and school staff could not access it any longer. On September 22nd it was announced that the hacker group had accessed large amounts of data, including CPR numbers (Danish personal identification numbers) and phone numbers, some of them belonging to minors.

According to some experts, the attack was one of the most serious cases in Denmark. The hackers were demanding a ransom of 5 bitcoins, equivalent to 1 million DKK.



NIS2 AND WHAT IT MEANS FOR CYBERSECURITY

The Long Awaited Upgrade

At this point it is old news, but this year NIS2 will finally move from being a theory to impacting everyday life of organizations, as Member States must transpose the Directive into applicable, national law by 17 October 2024. The European Directive requires Member States to adopt laws that will improve the cyberresilience of organizations within the EU and impacts organizations that are defined as “operators of essential services”. Under NIS 1, EU member states could still choose what this meant, but to ensure more consistent application, NIS2 has set out its own definition. Rather than making a distinction between operators of essential services and digital service providers, NIS2 defines a new list of the following sectors:

- *Energy*
- *Transport*
- *Public Administration*
- *Banking*
- *Financial Market Infrastructures*
- *Health*
- *Manufacturing Of Medical Devices*
- *Drinking Water*
- *Digital Infrastructure*
- *ICT Service Providers*
- *Postal And Courier Services*
- *Waste Management*
- *Chemicals*
- *Food*
- *Computers and Electronics*
- *Machinery and Equipment*
- *Motor Vehicles and Other Transport Equipment*
- *Digital Providers*
- *Space*



It is quite difficult to figure out if your organization does not fall under one of these areas, but with this new legal set-up it definitely becomes harder to try and find industry segments that won't be affected. As NIS2 represents legally binding cybersecurity requirements for a significant region and economy it focusses on essential and structural processes including mandatory incident reports with tight timelines. Under NIS2, affected organizations must submit an initial report or "early warning" to respective national authorities within 24 hours after a cyberincident. This major change in the law is meant to create more transparency as well as help the government to have a steeper learning curve when it comes to cyberattacks.

Accountability of the management

Another important addition to NIS1 is the accountability the new Directive assigns to the management of organizations in scope. The NIS2 Directive's revised penalties, reaching up to €10 million or 2% of an entity's annual global turnover, alongside individual managerial responsibility, set a standard. Penalties aren't just fairytales any longer. Especially with cases like former Uber CSO Joe Sullivan's sentencing, who failed to report a data breach, and charges against SolarWinds' ex-CISO Timothy G. Brown, who defrauded investors by overstating SolarWinds' cybersecurity practices and understated or failed to disclose known cybersecurity risks and vulnerabilities.

The law is clear on this issue; CISOs bear direct responsibility in cyberincidents. They have final oversight on assessing cybersecurity frameworks, team structures, and general IT security within their organizations. For their own sake as well as for the good of the organization they'll also look to join leadership teams who share similar values, hold themselves to a strong code of conduct, and who will support them rather than scapegoat them in times of crisis. Downplaying or under-reporting cyberrisk will lead to an economic disaster and companies might end up in the headlines for the wrong reasons.

Upgrade Your Security Stack

Many organizations, especially those that are newly in scope for NIS2, will have to manage and expand their information security risks. For organizations in this situation, there are various tools beyond the standard firewall and anti-virus software, a number of best practices, and frameworks that can be implemented.

The following responsibilities and key processes are defined under NIS2, such as:

- *Risk management and information system security policies*
- *Incident handling and management*
- *Business continuity and crisis management (back-ups, disaster recovery)*
- *Supply chain security*
- *Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure*
- *Policies and procedures to assess the effectiveness of cybersecurity risk management measures*
- *Cryptography and encryption, multi-factor authentication*
- *People, awareness and training*

Network Detection and Response in particular provides capabilities in the areas of network visibility, incident handling, and reporting that can help close the gaps in a cybersecurity stack.

AI and NIS2

Artificial Intelligence isn't specifically mentioned in the NIS2 framework. A reason for this might simply be the timing of the provisional agreement on NIS2 in May 2022 preceding the public awareness regarding broader AI technology, such as ChatGPT and other open-source Generative AI tools, by about six months. Had the law been drafted today, we might see more emphasis on AI, possibly even making it a requirement within the framework.

However, NIS2 does explicitly recommend the encouragement of innovative technologies, which signals a positive stance toward the use of AI. The Directive also emphasizes the importance of pro-active cybersecurity, defined as prevention, detection, monitoring, analysis, and mitigation of network security breaches.

Network Detection and Response which leverages AI can be a tool to proactively detect and respond to threats in real time, ultimately helping to have no disruptions in your network and secure data.

Moreover, a NDR gives full visibility to ensure policy effectiveness and compliance within the NIS2 framework. The Directive covers incident handling and business continuity as well as reporting of cyberincidents, which plays a crucial role plays in handling future cyberattacks, as we are only able to learn from the current ones. It seems like a simple task, but with the amount of network data we are producing today proper reporting tools are innovations that don't get so much attention. Detailed and comprehensive incident reports will not only be quickly generated, but also contain all relevant information without wasting much time.



What Can We Expect

How exactly the different EU member states will implement NIS2 into their national laws remains unclear, with the deadline for this process set at October 17, 2024. In addition, the European Union pledges to assess the effectiveness of the Directive every three years.

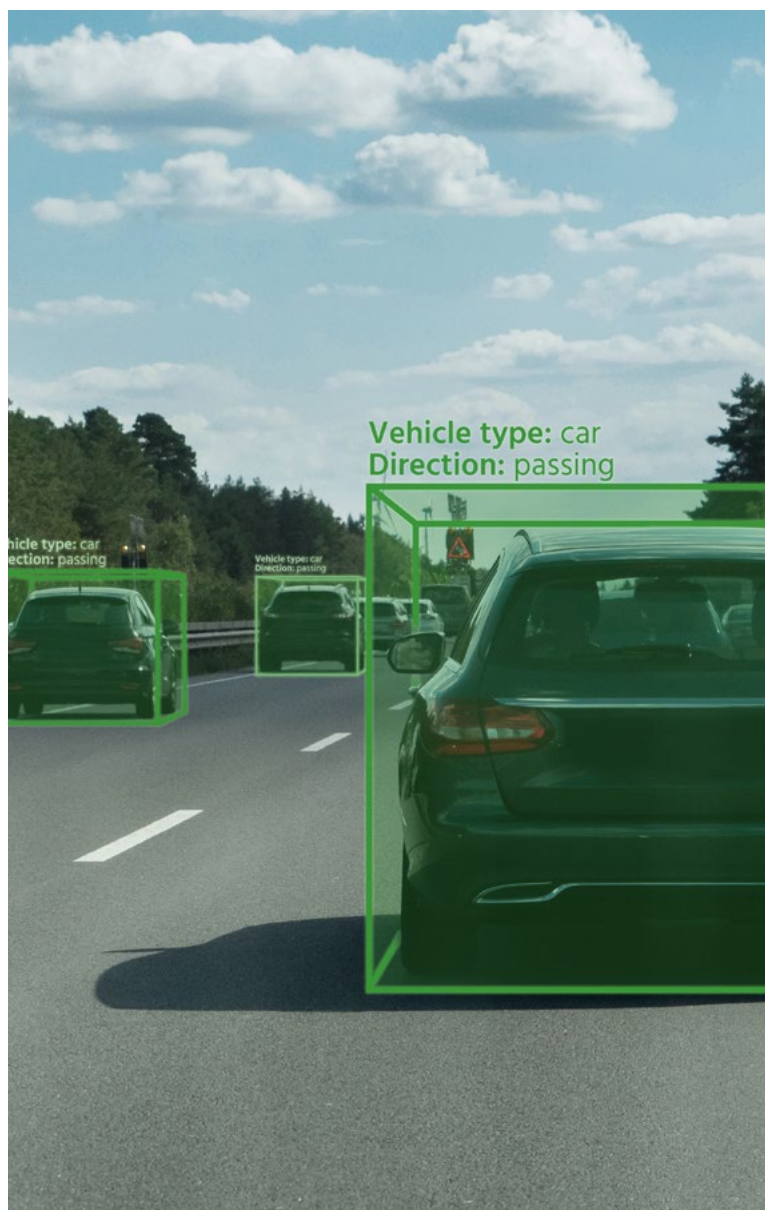
Considering the technical milestones, we have made over the last twelve months and recognition of both the risks and potential indispensability of AI, particularly within cybersecurity, we might come to a point where numerous member states might make AI mandatory to counteract growing cyberthreats and the lack of IT staff available.

THE CRITICAL CHALLENGE OF AI SECURITY

A New Risk Profile

The era of rapid AI development, also known as the AI Spring, is pressuring companies to shorten their Time-to-Market drastically. In order to stay competitive, they rush to release AI-based products, often sacrificing thorough development and testing. This rush results in underdeveloped AI systems that lack robustness and reliability. New machine learning (ML) algorithms, which are crucial to these developments, may enter production without adequate large-scale review, increasing the risk of ineffective or potentially hazardous implementations. The lack of software development resources increases these risks and challenges even further. Today's high demand for AI expertise significantly outweighs the supply of skilled professionals and the high costs of computational resources, like GPUs, reduces the general access to AI models. The situation gets even trickier because of data quality, where training data does not meet the expectation and need for high-quality and relevance, resulting in weak AI outputs.

A study from UC Berkeley in Adversarial Machine Learning (AML) showed how AI systems can be tricked by simple environmental changes. Researchers demonstrated that self-driving cars could be tricked into incorrect actions by merely placing stickers on the road. This experiment underlines the sensitivity of AI systems to minor manipulations and shows the importance of designing AI with a higher level of resilience against such interference. For further details, [Berkeley's CLTC website on AML](#) offers more information.





What is Adversarial Machine Learning?

Adversarial Machine Learning (AML) is a concept that sits at the intersection of cybersecurity and AI. It addresses the issue of adversarial attacks, which exploit the weaknesses in AI solutions. AML focuses on understanding and reducing the vulnerabilities inherent in AI systems, providing strategies and methods to defend against such attacks. This field is becoming increasingly important as AI systems become more mainstream and are being integrated into various aspects of technology and daily life.

Understanding and defending

against adversarial attacks is essential for ensuring the reliability and safety of AI applications.

How does an AML Attack Work?

Because ML models are data-driven, adversarial ML attacks introduce unique security challenges during model development, deployment and inference.

AML attacks can be categorized into two main types: white-box attacks and black-box attacks. In a white-box attack, the attacker has extensive knowledge about the ML model, including its underlying architecture, training data, and the

optimization algorithm employed during training. This deep understanding enables the attacker to execute highly targeted exploits.

On the other hand, in a black-box attack, the attacker lacks or has limited knowledge about the ML model, including its architecture, training data, decision boundaries, and optimization algorithm. Consequently, the attacker must engage with the ML model as an external user, using a trial-and-error approach through prompts to uncover vulnerabilities by analyzing its responses.

In general AML focuses on four main threats: Evasion Attacks, Poisoning Attacks, Extraction Attacks, and Inference Attacks.



Evasion Attacks

These occur during a model's testing phase, where attackers modify inputs to cause incorrect predictions. These subtle changes are hard to detect but can significantly mislead the model. In this context, the case of the Cylance INFINITY AI engine presents a notable example. Cylance INFINITY AI used a scoring mechanism ranging from -1000 to +1000 to evaluate files, with certain executable file families whitelisted to minimize false positives (FP). This approach inadvertently introduced a bias towards code in these whitelisted files. Exploiting this vulnerability, researchers conducted an evasion attack by extracting strings from an online gaming program that was on Cylance's whitelist. They then appended these strings to malicious files, specifically the WannaCry and Samsam ransomware. As a result, the Cylance engine misclassified these altered ransomware files as benign, shifting their scores from high negative to high positive. The research findings were presented at "BSides Sydney 2019".

Poisoning Attacks

Targeting the training phase, these attacks involve injecting harmful data into the training set, leading to a corrupt and poorly performing model, posing serious security risks. A notable instance is altering training images for self-driving car algorithms, where manipulated stop signs images caused misidentification of road signs, demonstrating severe real-world implications of such attacks.

Extraction Attacks

Attackers reverse-engineer a model to extract crucial details like its structure or training data, compromising its integrity and enabling more targeted subsequent attacks. Recently, researchers have demonstrated the feasibility of model extraction attacks in adversarial machine learning, showing that it's possible to reverse-engineer machine learning models. In this context, there are examples indicating that even sophisticated image analysis systems are susceptible to such security breaches.

Inference Attacks

These attacks analyze a model's outputs to infer private data, posing a significant privacy risk, especially with sensitive information like medical or financial records. The case of the Netflix Prize serves as a significant example of an inference attack. When Netflix released an anonymized dataset for a competition aimed at improving its recommendation algorithm, researchers found a way to de-anonymize part of it. They achieved this by comparing the Netflix data with publicly available IMDb movie ratings, allowing them to identify certain Netflix users.

We've
conve
ChatG
challe
reque
trained
detail



**EVOLVING SECURITY
STANDARDS FOR
THE POST-QUANTUM
CRYPTOGRAPHY ERA**

TOMORROW'S LOCK AND KEY

The Purpose of Post-quantum Cryptography

Why is post-quantum cryptography (PQC) important? Well, it's all about safeguarding your sensitive data in the face of future quantum computing advancements. As traditional encryption methods might become vulnerable – and quite frankly redundant –, post-quantum cryptography steps in to make sure your data remains secure.

What is Quantum Computing?

Simply put, quantum computing's immense potential to revolutionize speed and processing power of computers also poses a serious threat to existing cybersecurity. Many experts and scientists now believe it to be merely a significant engineering challenge and that it could unravel our current encryption methods, leaving our sensitive data exposed.

Post-quantum cryptography is a part of the efforts to ensure we will have quantum-secured technologies before 'Q-Day' – the point at which quantum computers are able to break existing cryptographic algorithms. These efforts include various evolving techniques aimed at keeping data private, from personal passwords to bank details or crucial access to sensitive facilities. Without this safeguard, the world as we know it, reliant on secure information and access, would be at risk of functioning.

Public-key Encryption

The challenge humanity faces lies in our reliance on pre-quantum cybersecurity built on public-key technology.

Public-key encryption is a cryptographic method that uses two keys, a public key and a private key, to secure communication over insecure channels. Each user has a pair of keys: the public key, which is freely distributed and used to encrypt messages, and the private key, which is kept secret and used for decryption. Messages encrypted with a recipient's public key can only be decrypted using their corresponding private key, ensuring confidentiality and authenticity in digital communication. This technology is the backbone of secure online transactions, data transmission, and confidentiality in any online space.

Essentially it is like twenty linked Rubik's cubes: altering one affects all, yet each starts with a different configuration. Solving these puzzles collectively demands significant computational skills and time—time crucial for security teams to detect and thwart potential hackers while alarms blare. This works well when everyone uses similar computers, maintaining a balanced playing field.

However, the impending speed of quantum computing arises from

its ability to handle enormous computations and numbers simultaneously. Unlike traditional systems, quantum computing's unparalleled capacity threatens to decode these encrypted data sets before you can even start a countdown, making passwords basically irrelevant.

The Theory

That's the theory, at least. We can't know for sure if quantum computing will indeed achieve that. If the apocalyptic scenario of quantum computing decrypting everything secured by public-key encryption becomes a reality, we'll feel quite foolish for a hot minute right before the world plunges into chaos and a primitive, non-computer dystopia.

Besides public-key encryption; there's also the individual-specific private-key. In short, private-key encryption employs a single key for both encrypting and decrypting messages. This shared secret key is used by both the sender and recipient to encode and decode information. It's efficient for secure communication between trusted parties but requires the key to be securely exchanged beforehand. Private-key encryption is commonly used for secure data storage, in VPNs, and for securing sensitive information within closed systems.

However, widespread belief suggests that if quantum computers crack public-key cryptography, the private-key

encryption will likely be a simple warm-up before moving onto the more complex challenges.

It is urgent that we counter-develop to prepare for the quantum computing era by adopting post-quantum cryptography. But what exactly is the purpose of post-quantum cryptography? What does it entail and how can we implement it?

The Science

The functioning of post-quantum cryptography depends on understanding its possible purpose and guessing right what quantum computers will be capable of.

Basically, pre-quantum public-key cryptography typically relies on three mathematical problems: the integer factorization problem, the discrete logarithm problem, and the elliptic-curve discrete logarithm problem. A more in-depth explanation on this can be found online.

Post-quantum cryptography will most likely still revolve around public-key methods at its core. However, the aim is to only focus on a selection of alternative techniques. This shift arises from the anticipation that quantum computers will easily overcome existing security challenges using algorithms like Shor's algorithm, which is used to solve the three above mentioned mathematical problems.

Potential Post-Quantum Cryptography

Historically, it has taken almost two decades to deploy our modern public key cryptography. A transition from current cryptographic standards to quantum-safe alternatives won't happen overnight. So, if we were to establish a new system, we had better start the process already. Hence why, in 2016 the National Institute of Standards and Technology (NIST) launched a competition aimed at identifying and establishing the most robust post-quantum cryptographic algorithms.

Picture it as a showdown where encryption techniques vie against quantum adversaries to showcase their efficacy. These algorithms undergo meticulous examination and trials to eliminate the ones not being able to withstand the decryption-attacks.

There is a range of public-key algorithms that promise to offer post-quantum cryptography:

Lattice-based ^a

Lattice-based cryptography stands out in this domain. Specifically, NTRU lattice-based cryptography, a public key cryptosystem, has gotten some attention due to its extensive testing on current computers, and its resilience against years of decryption attempts. Particularly a variant known as the Stehle–Steinfeld version, is being called a potential frontrunner for post-quantum cryptographic standards by the Post Quantum Cryptography Study Group and the European Commission

Hash-based cryptography

Hash-based cryptography has existed since the 1970s, leading some to believe it might be inadequate against future quantum computer threats in the 2020s or 2030s. However, their inherent nature as substitutes for numerical digital signatures could have a significant relevance in post-quantum cryptography. While it currently receives less attention

compared to lattice-based cryptography, there's potential for evolved versions of signatures like Lamport or Merkle to contribute significantly to the post-quantum era.

Supersingular elliptic curve isogeny cryptography

This tongue twister, supersingular elliptic curve isogeny cryptography, could indeed offer advantages in terms of forward secrecy, particularly in evading mass surveillance by hostile governments. It essentially presents a quantum-resistant adaptation of the already extensively used public-key cryptography version, the elliptic curve Diffie-Hellman key. This makes it a promising and minimal-effort upgrade.

Symmetric key quantum resistance


An existing alternative that's already in practice: symmetric keys. While public-key cryptography differs from symmetric key

cryptography, the latter is currently in use and anticipated to resist quantum intrusion. Consequently, numerous organizations propose a complete substitution of public-key cryptography with symmetric key cryptography.

But this will stay a theory only until we are able to determine whether this shift will offer a lasting solution until post-quantum cryptographic algorithms undergo testing with quantum computers in practical settings.

Code-based cryptography

Another prospect endorsed by the European Commission; code-based cryptographic algorithms often depend on error-correcting codes. Interestingly, the McEliece signature algorithm has defied decryption attempts for over four decades, leveraging random codes. Attempts by researchers to impose more structure on the McEliece signature consistently led to reduced strength and stability, implying that valuable randomness might have a significant role in



post-quantum cryptography.

Multivariate cryptography

Considered a bit of a gamble in the current group of solutions, multivariate cryptography operates precisely as its name suggests—using cryptography founded on solving multivariate equations. However, its current iteration hasn't demonstrated notable effectiveness in testing. The principle of making public-key cryptography slightly more intricate might not endure beyond a few iterations in the face of fully operational quantum computers, at least in its current form.

In July 2022 and after several rounds of selection, NIST announced the four encryption algorithms, three of them being Lattice-Based and one being Hash-Based, that would form its PQC standard. The CRYSTALS-Kyber algorithm was chosen for general encryption (access to secure websites) and CRYSTALS-Dilithium, FALCON and SPHINCS+ were selected for digital signatures.

NIST then requested the industry's feedback on the draft documents before November 2023 and we are expecting that the standards will become the global benchmark for quantum-resistant cybersecurity across the world in 2024.

Currently the concept of employing more intricate mathematical approaches has its appeal. Even if, for instance, the apocalyptic scenario of quantum cryptography doesn't unfold as dramatically as some of us predict, post-quantum cryptography might still carve out a future with stronger cybersecurity.

But regardless of the algorithms that best withstand the power of new quantum computing, they will undeniably shape the trajectory of corporate, governmental, and personal cybersecurity for at least a generation. As identifying these options remains somewhat of a speculation for now, Muninn will keep a close eye on the development as it certainly will have a major impact on future-cybersecurity.

FROM REVOLUTION TO EVOLUTION

An excited buzz spread within the tech community throughout 2023 as a number of technological milestones and new AI tools made the headlines. Over the last twelve months Artificial Intelligence sparked conversations across industries and has set a new era in motion.

It is almost too obvious that 2023 will be remembered as the year generative AI emerged, tools trained on vast datasets that create outputs based on various prompts. [McKinsey's annual survey](#) showed a staggering 79% exposure to generative AI among respondents, with 22% of them confirming regular use of AI tools. Some highlights made this a very transformative year:

OpenAI's launch of a subscription-based model of ChatGPT, empowering third-party developers to seamlessly integrate ChatGPT and Whisper (voice-to-text-model) into applications such as Home Assistants through a pay-per-use API. Their introduction of GPT4, a more robust and advanced large language model (LLM), reinforcing the evolution of AI and broadening ChatGPT's capabilities by incorporating image processing.





AI might help find new cures in medicine. NVIDIA has broadened its product portfolio with the introduction of BioNeMo, a sophisticated AI-driven platform intended to predict the structures of proteins, a crucial step in accelerating the development of new potential drugs. Additionally, NVIDIA has expanded its collaboration with Microsoft, aiming to streamline accessibility to its products for users on the Azure platform.

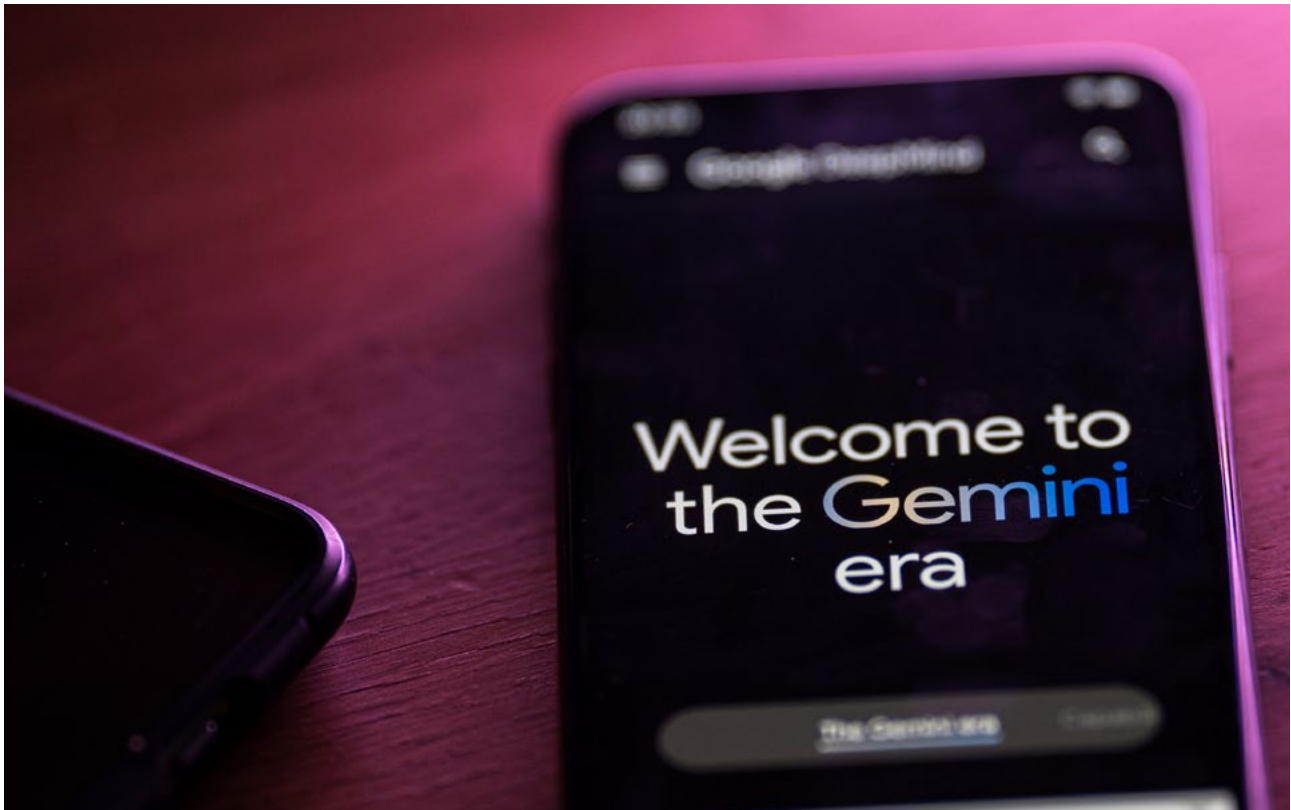
Meanwhile, [AWS](#) has launched an ambitious initiative named 'AI Ready', a free of charge, online training program aimed at helping both tech-nerds and non-tech professionals with fundamental skills essential for careers in generative AI. This initiative not only addresses the pressing shortage of skilled AI professionals but also sets a goal to train up to 2 million individuals by 2025, paving the way for current and future workforce needs. On top of that, AWS is rolling out scholarship programs to promote AI education in high schools and universities worldwide.

Google's release of Bard, its chatbot designed as a counterpart to ChatGPT, while Microsoft announced plans to integrate ChatGPT into its product lineup. Not to be outdone, Google introduced PaLM2, an advanced LLM intended as a direct competitor to OpenAI's GPT4, making it a heated generative AI race.

Meanwhile, HeyGen was celebrated in social media circles, using generative AI to empower video content creators. This groundbreaking service allows creators to create avatars resembling themselves and generate video content and translations of it in numerous languages, all in the creator's own voice. Impressively, HeyGen automatically adjusts facial expressions and lip movements to synchronize with the translated content, revolutionizing content localization.

But some of this year's advancements come as an answer to certain concerns. MIT researchers developed PhotoGuard, a pioneering tool capable of encoding photos with unique tags to prevent non-consensual deepfakes. By tricking AI models into using incorrect information for image generation, PhotoGuard offers a safeguard against misuse of visual content. The University of Chicago presented Glaze, a tool designed to detect and encode an artist's distinctive style into photos. These encoded images deter or prevent mimicry of the original artist's style, making a significant step in development to protect artistic integrity in the digital world.

Looking ahead, 2024 will not put a hold on the development and we will continue to see a numerous creation of AI tools, although their pace of development and adoption might face some obstacles due to hardware shortages and legal concerns surrounding the use of AI and its outcomes. The impending enforcement of the EU AI Act in 2024 sets a ticking clock for businesses involved in AI systems or components, potentially forcing them to align with the regulations rather sooner than later ■



THE RISE OF VERSATILE AI AGENTS

Beyond Words and Pictures

When you scratch beneath the AI surface, it's clear the hype will soon evaporate. LLMs are typically quite difficult to use, because they are unable to understand context or provide reliable outputs, which restricts the wider use. This year we might therefore see businesses scale back their use of LLMs.

As current tools will become more functional and user-friendly, the next generation of generative AI (Gen AI) tools will go far beyond the chatbots and image generators that have amazed and sometimes scared us in 2023. This next wave will show multifaceted capabilities beyond textual interaction. Multimodal AI tools adeptly comprehend and process information from diverse data types like images, videos, audio, and more. Such advancements enable engineers to build AI agents tailored for a spectrum of tasks, while LLM-powered agents mostly facilitate uninterrupted back-office operations.

For instance, ChatGPT's voice feature streamlines tasks by eliminating manual typing. Users can articulate

commands while the LLM retrieves summaries, generates charts, devises fiscal plans, and more. With Gen AI alleviating daily tasks, we as humans can redirect our focus towards strategic and innovative projects.

Google's Gemini, a multifaceted AI launched in December '23, sets out to seamlessly reason across text, images, video, audio, and code. This product is meant to bridge the gap between Google and OpenAI. While Gemini launched with robust benchmarks and a captivating video demonstration, a closer look revealed flaws, leaving critics with more questions than answers.

As AI applications will most likely grow in complexity, ensuring oversight of these AI tools becomes increasingly important. Having people with knowledge to analyze and debug will be essential in handling risks such as errors and AI's biases in planning, task execution, and reflection processes. Human supervision will remain an integral part of solving these issues. Simultaneously, establishing responsible Gen AI principles throughout the developmental is a necessary and critical imperative.



DEEPFAKES

From Fiction to Reality

With the upcoming U.S. election, we will most likely see an increase in manipulated videos, portraying politicians or others saying things they never did, posing a significant concern for consumers and voters alike. Legislative actions are on the horizon, notably within the EU, where the final EU AI Act will start to have its first impact in 2024. However, we still don't know how this will affect major American tech companies and their AI models. We might see some states implementing laws, but overall, we might not see any significant regulation in the U.S..

Our expectations for 2024 include a surge in startups and companies like OpenAI unveiling larger AI models, with a wide range of new functionalities. Nonetheless, the debate surrounding AI and its definition will not be closed, overshadowed by concerns about current challenges like disinformation and the spread of deepfakes. While fears of AI dominating the world are more Hollywood material and conspiracy hype, our imminent focus should remain on addressing the present harms inflicted by disinformation and manipulated media.

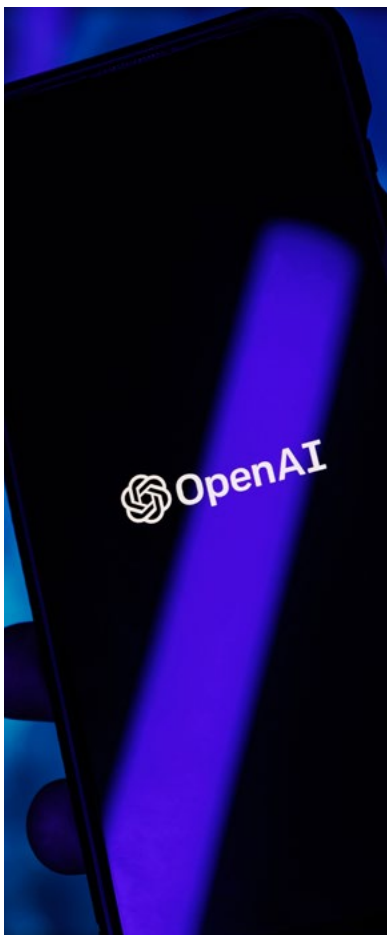
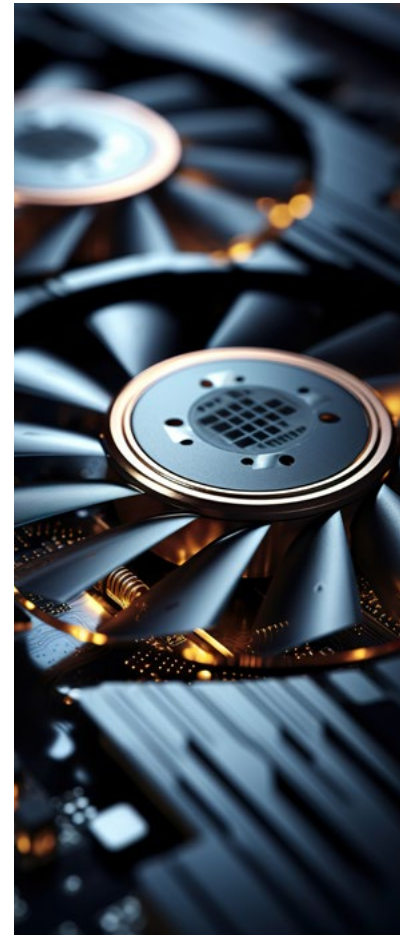
CHIP CRISIS

The High Demand for GPUs

We are used to high-speed internet connections and applications running smoothly that we hardly think about the hardware needed for it. GPU processors are essential to AI operations and as more companies seek AI capabilities, an unprecedented demand for GPUs, primarily produced by companies like NVIDIA, will emerge, potentially limiting availability. The scarcity of GPUs will not only impact companies' competitiveness but will also impact organizations developing AI innovations.

Consequently, we will see a higher pressure on increased GPU production and for innovating more cost-effective and user-friendly hardware alternatives. Ongoing research in electrical engineering at Stanford and other institutions are already exploring low-power substitutes for existing GPUs.

It might take a while to get from a research phase to a widespread availability of such a solution, but the focus on accelerating such developments is crucial in order to keep democratic access to AI technologies.



The Democratization of Coding with Low-Code and No-Code Software Engineering

In 2019, [Gartner](#) foresaw a surge in low-code/no-code tools dominating 65% of app development by 2024. This prediction aligns with the rise of generative AI tools such as ChatGPT, enabling app creation and testing within minutes. While coding and software engineering roles won't disappear, because someone needs to develop these AI tools, 2024 will present a great opportunity for creatives that like to solve problems but lack those necessary technical skills.



AI's Binary Impact on Cybersecurity

AI has undeniably transformed the lives of high school students, simplifying writing essays and helping with homework, but regrettably, it has also empowered cybercriminals. The increasing number of AI-generated code for hacking in 2023 marked a concerning trend and is likely to intensify in the upcoming months.

One concerning innovation that has gotten some attention in online forums is WormGPT, a LLM trying to copy ChatGPT but without any ethical safeguards and made for malicious intent. The tool has been reportedly used to help facilitating hacking campaigns and is a significant leap in the arsenal of cybercriminals.

Once a LLM is built to execute whatever malicious prompt the issue lies in the speed and volume of scams such an AI language model produces, especially when used as a weapon by professional hackers. We have all seen the speed at which these models generate text and how they easily replicate certain recipes. Now imagine this output being cyberattacks like phishing emails or malicious code, even criminal first timers are able to create.

But ChatGPT poses a security risk from within organizations too. The rush of blindly using LLMs in whatever integrations or form at work, isn't without risks. It has been reported that these hyped AI tools lack data privacy standards and hackers might even be able to simply get your company's internal data, in case an employee has been feeding it to the LLM. A data leak without any network infiltration at all.

But there is hope in the form of a two-way trend. AI has been an established part of cybersecurity for years and as we move into 2024, there's an expectation for AI to evolve and grow with our challenges. Organizations are already adapting by integrating machine learning tools into their SOC platforms and set-up.

It seems like a cybertale as old as time, but the solution lies in proactive measures. IT security professionals must focus on reducing breaches caused by AI-generated code, by rigorously monitoring their networks for any abnormalities. Moreover, organizations need to establish clear policies on approved AI tools and their proper usage to

ensure compliance with existing data privacy and cybersecurity standards.

Looking ahead, vigilance is key. Predictions suggest a surge in cybercriminals exploiting AI and outdated security measures. There's also a looming threat to Managed File Transfer systems and file servers, making them lucrative targets. Strengthening defenses is imperative, especially against potential future attacks like torrents, which facilitate the release of sensitive information.

One defense strategy that has proven its effectiveness involves understanding your network activity and user behavior within your organization. By closely monitoring expected user behavior, slight anomalies can indicate a security breach. For instance, a sudden and unusual amount of data being uploaded could raise red flags signaling a potential threat.

Something AI can already detect today, and we expect it to be even more nuanced in the future to identify the stealthiest hackers.

NEW RULES

The EU's AI Act

Ethical, legal, and socio-political questions regarding AI will only get more complex and difficult. As a result of political discussions and decisions in 2023, the EU's AI Act is set to come into effect in the first half of 2024, being a monumental step in regulating the entire spectrum of AI development, distribution, and deployment within the EU. This new legislation adopts a risk-based approach, categorizing AI practices into unacceptable, high-risk, limited-risk, and minimal or no-risk tiers, each subjected to varying degrees of regulation. With non-compliance fines, reaching up to EUR 30 million or 6% of global turnover, companies will face significant challenges, big AI players and newbies on the market alike.

The new year will also manifest the need for international collaboration on AI safety. While the EU spearheads AI legislation, countries like the US and UK have addressed this issue in a different way. The

Biden administration's Executive Order in October 2023 outlined a holistic approach in order to build trustworthy AI, coinciding with the UK-hosted international AI Safety Summit that resulted in the Bletchley Park declaration, signaling the beginning of some collaborative efforts on the matter. Notably, the UK and other nations announced measures surrounding AI regulation during and around the summit, setting the stage for further discussions and potential summits dedicated to AI regulation and safety. Knowing the usual pace of the political apparatus, the development of new technology might already make it to the finish line before politicians know which distance they will need to run. Trying to keep up, two AI Safety Summits are already planned for mid and end of this year, where 28 countries, including the United States, China, and the European Union, will follow up on recent developments.





So, what now?

There is no doubt that generative AI will transform the cybersecurity landscape in significant ways. But as we step into 2024, our outlook for AI and how it will affect the rest of the world remains optimistic. 2023 was one big hype, but we will be a little less delusional and more focused going forward. The year ahead will be the birth of several new AI models with a diverse number of capabilities, presenting new risks as well as great opportunities. Cost considerations, limited production of hardware and regulatory policies will have a substantial influence over enterprise adoption of AI tools, steering the course of the general integration and impact of AI in organizations. As the year unfolds, navigating these developments will undoubtedly shape the impact of AI's role in driving innovation and efficiency across industries and especially within cybersecurity.

BEYOND THE HOODIES

Decoding the Realism of Hacking in Hollywood

The headlines in the news are filled with cybercrime, whether it is government online services being disabled or a company's data leaked. Hollywood has foreseen this future for decades. With popular TV shows like Mr. Robot and Black Mirror having gotten more attention over recent years, the topic of cybersecurity also takes center stage in pop culture. However, Hollywood has its own perspective on it and is known for dramatizing cybersecurity scenes. We all have seen scenes that often include suspenseful music and hundreds of people, including the president of the United States, panicking about a firewall being hacked.

Despite well researched tv shows such as "Mr. Robot" are and interesting a lot of these scenes may seem, they're out of touch from reality, and hardly represent what it's like. By default, movies and TV shows are designed to keep the viewer engaged, and even as IT professionals, we can't take our eyes off the screen when these scenes appear on our television.





Don't Believe Clichés

Hollywood is known for their tropes, which are sometimes exaggerated to fit a specific stereotype or narrative in order to appeal to the viewer. Let us look at some of the commonly used stereotypes that Hollywood uses to entertain us or make some of us roll their eyes once in a while:

Multi-System Hacking

The most common stereotype of hacking in movies is multi-system hacking into an entire company's or government institution's systems. This is rarely the situation outside of Hollywood. In fact, human error is responsible for 82% of cybersecurity breaches, and phishing emails are one of the most common cyberattacks affecting businesses. But employees accidentally clicking on an email they shouldn't have or leaking private data to someone they believe is their manager doesn't make for a box office hit movie.



It Takes a Second for your Network to Recover

Movies make it appear that a cyberattack can be resolved in less than an hour with a few lines of code – and we wish that was true. However, these attacks take an average of 277 days (9 months) to identify, and some businesses never recover due to a lack of a recovery plan in place.



Only Big Organizations can be Attacked

When you watch these movies, you may believe that small to medium-sized businesses are safe. However, when it comes to avoiding cyberattacks, bigger is apparently better. At least that's according to a new report that shows small businesses are three times more likely to be targeted by cybercriminals than larger companies. Between January 2021 and December 2021, researchers analyzed millions of emails across thousands of companies. They found that, on average, an employee of a small business with less than 100 employees will experience 350% more social engineering attacks than an employee of a larger enterprise.



Coding is the only way to protect yourself from cybercriminals

In movies and TV shows, we often see dramatic scenes of frantic typing and key slamming as a last-ditch effort to prevent cybercriminals from infiltrating networks and causing disruptions. Movies like "Swordfish" entertain us with scenarios where hackers perform their tasks under extreme circumstances. However, this reactive approach, where organizations respond only after a breach has been detected, is far from the ideal strategy.

In the real world, such a reactive approach is inadequate, primarily due to the lengthy process of identifying the root cause of a security issue, which can span weeks. Prevention is key and consistent threat hunting a tool to avoid crisis management.



Add to Playlist

The importance of IT professionals and the global awareness of the lack thereof have underlined the current and future demand for cybersecurity talent. The world is increasingly dependent on the knowledge and skills of technology experts, a shift that might have been unexpected in the past but is hardly a concern in Hollywood's futuristic portrayals.

To dive deeper into Hollywood's view of cybersecurity, let's take a closer look at certain portrayals available on your Netflix or other streaming services' playlist.

Ghost in A Shell – 1995

Dial-Up Days of Digital Derring-Do

Ghost in the Shell is a Japanese animated cyberpunk film directed by Mamoru Oshii. The movie takes the viewer into a future where humans can augment their bodies with cybernetic enhancements. The story follows Major Motoko Kusanagi, a human-machine hybrid whose construction is shown during the film's opening credits, as she investigates a mysterious hacker known as the Puppet Master, who can hack humans as well as machines. The film takes place in a near future in which humans have begun to merge with machines. Limbs are upgraded with weaponry and other special functions; eyes are replaced with powerful computer-enhanced sensors; minds and memories are expanded via external storage technology.

Director Mamoru Oshii wanted a piece that portrayed the "influence and power of computers" by looking at how this influence and power might evolve over time. The movie has had a significant influence on the sci-fi genre, inspiring numerous works that explore the intersection of technology and humanity. It also has been recognized for its philosophical depth, stunning visuals, and pioneering role in the anime industry.

2 Mr. Robot – 2015-2019

Hacking, Hoodies, and a Dose of Reality

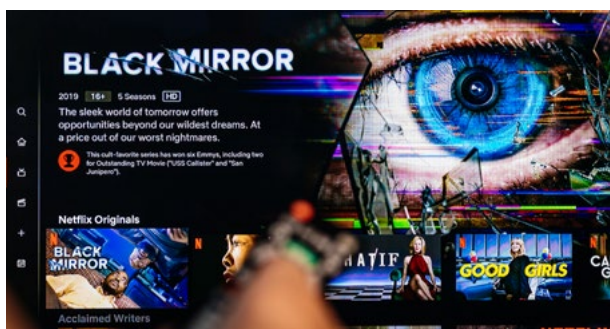
The series, which aired for four seasons between 2015 and 2019, followed Elliot, portrayed by Emmy winner Rami Malek, who was a singularly talented man—a hacker so disconnected from modern life and anyone else that functioning in most social situations seemed beyond his reach.

“Mr. Robot” was all about hacking and thus filled with scenes of someone typing furiously at a computer, which back then had been a showstopper for realistic drama. But Sam Esmail, the mastermind and creator of the show, knew about coding, and thus hacking, and so each episode felt real. It wasn’t just typing. The voiceover that was being used was essential, adding layers to the complex coding. It sped up adrenaline and made the typing dramatic.

3 Black Mirror – S06 – 2016

Social Media Meets Human Clone and Cybercrime

Across six seasons, Black Mirror has fearlessly explored a spectrum of technological dilemmas, diving deep into everything from artificial intelligence to cyber-clones. Its latest season adheres to the familiar yet introduces new elements. Unlike its past focus on technology’s havoc, this time, it probes society’s self-inflicted scars. Season six proves that the creators of Black Mirror excel in its dystopian narratives and that tinkering too much with this successful formula might impact the show’s future success.



4 Sneakers – 1992

Espionage with a Side of Wit

Sneakers, directed by Phil Alden Robinson, blends thriller, comedy, and heist elements in a post-Cold War setting, following a San Francisco-based counter-security team stumbling upon a device with the ability

to crack any U.S. government code—an almost futuristic concept. Or not so much? Penned by Lawrence Lasker and Walter F. Parkes, known for “WarGames,” the film echoes concerns about government perils intertwined with technology. Yet, amidst these themes, there’s an undeniable fascination with the allure of this technological prowess.

The movie is a place where technology remains both captivating and a touch nerdy, as highlighted in the portrayal of Stephen Tobolowsky’s character as a ‘computer dater,’ evoking a slightly forlorn sentiment. “Sneakers” offers a retreat to a somewhat familiar realm—a world where technology is awe-inspiring yet devoid of the modern digital chaos we’ve grown accustomed to today.

5 Hackers – 1995

Cyberpunk Rebels and Outlandish Outfits

The standout feature of Hackers is its distinctive style. This 1995 tech-crime thriller, led by Angelina Jolie, ventures to portray a genuine phenomenon through a flashy and intricate lens. However, the movie’s attempt to fictionalize reality has a mixed outcome. From the get-go, the improbable scenarios and heavy technobabble easily feel like a cartoonish portrayal of hacking—an escapade tailored for ‘90s adolescents who were embracing the idea of empowerment through taking control.

Yet, much like real hacking isn’t just frantic typing amid cascading numbers, Hackers isn’t merely a subpar tech movie. It has reached an almost cult classic status and is highly embraced for its unique visuals. While the hacking itself might not align with reality, the film creates a captivating world and is undeniably entertaining. For many fans of Hackers, this entertainment value is more than sufficient to appreciate and enjoy Hackers.

It is obvious that Hollywood’s representation of cybersecurity and hacking over the last few decades has often deviated from reality, yet it has also served as a reminder of technology’s dual essence: it both empowers and entertains us while presenting inherent risks and complexities.

In a world increasingly reliant on technology, these movies and TV series become catalysts for discussions concerning the ethical ramifications of our interconnected digital existence. Although they amplify situations for effect, they are able to spark dialogues essential for comprehending the evolution of current or future technologies ■

The Next Generation of Cybersecurity

Often in life – and in cybersecurity, we find ourselves at a crossroad. Being visionaries, we aspire to be at the forefront of Network Detection and Response. I see the current challenges, such as continuous shortage of cybersecurity professionals, not only as obstacles but as a driver for innovation and change.

Cybersecurity has reached a critical moment where the lack of skilled personnel is becoming more apparent, all while attacks increase. One of my big concerns is the gap in expertise, which is not merely about having fewer hands on deck but also about the varying levels of competency within the cybersecurity workforce.

The next generation of NDR must try and push the traditional boundaries of cybersecurity, to not only fill the lack of IT-staff but to educate users. Our products need to evolve into sophisticated tools without increasing complexity. On the contrary, they should reduce time spent on implementation and threat investigation. Imagine NDR 2.0 and how it will adapt to the user's knowledge level, guiding them through the complexities of all network activity with intuitive ease.

But it isn't just enough to respond to changes; real innovation comes from a leadership mindset. The way we, at Muninn, see the future of NDR is as a hub of learning, and a tool of empowerment. We commit to developing solutions that are not only setting new standards but also keeping the focus on the needs and challenges of users in focus.

As we move ahead, our focus remains steadfast on innovation, education, and adaptability. Cyberthreats and hackers will continue to evolve, and so will we. Muninn is not just about creating advanced NDR platforms; we want to help shape a future where everyone, regardless of their skill level, can contribute effectively to a better cyberdefense. This is more than a mission; it's our responsibility and our promise to the future.

A portrait of Uffe Damtoft Pedersen, a middle-aged man with short, light-colored hair, wearing a dark blue blazer over a white button-down shirt and dark trousers. He is standing against a background of vertical wooden slats. His hands are in his pockets, and he is looking directly at the camera with a neutral expression.

**UFFE
DAMTOFT
PEDERSEN**

**Keeping a sharp
focus on innovations
and tomorrow's
cybersecurity
solutions.**

⟨o⟩ Muninn

info@muninn.ai +45 70 60 59 08 www.muninn.ai

Copyright © 2024 by Muninn