Macrothink Institute™

International Journal of Regional Development
ISSN 2373-9851
2024, Vol. 11, No. 2

Bridging AI Innovation and Cybersecurity: Generative AI's Contribution to NIS2 Compliance

Dr. Christos P. Beretas, MSc. Ph.D

E-mail: c_beretas@yahoo.com

Dr. Athanasios Davalas, Ph.D

E-mail: adavalas@aegean.gr

Received: December 2, 2024 Accepted: December 16, 2024 Published: December 19, 2024

doi:10.5296/ijrd.v11i2.22486 URL: http://dx.doi.org/10.5296/ijrd.v11i2.22486

Abstract

The digital world is changing quickly. One big area of focus is how artificial intelligence (AI) fits in with cybersecurity. New rules, like the **NIS2** Directive, are pushing organizations to keep their systems secure. This research looks at how generative AI can help meet those safety standards. More companies are using generative AI for things like data creation and risk assessment. This gives them a chance to improve their security practices. We explore how AI tools, like machine learning and natural language processing, can help find weaknesses, predict threats, and respond to incidents. This way, companies can follow the tough rules set by **NIS2**. We analyze how AI is currently used in cybersecurity. The goal is to share best practices for using these technologies well. We also address the challenge of keeping new tech secure. In the end, we want to add to the conversation about AI and cybersecurity. We give advice for policymakers and business leaders on how to use generative AI as a smart tool for both innovation and meeting **NIS2** requirements. This study highlights how generative AI can help improve cybersecurity while also fulfilling regulatory needs in today's tricky digital landscape.

Keywords: AI Innovation, Cybersecurity, Generative AI, NIS2 Compliance, Artificial Intelligence, Cybersecurity Frameworks, EU Cybersecurity Directive, Risk Management, Data Protection, Compliance Strategies, Machine Learning, AI in Cybersecurity, Security Standards, Digital Infrastructure, Threat Detection, Incident Response, Cyber Resilience, Technology Governance, Innovation in Cyber Defense, Regulatory Compliance, Cyber Threat Landscape, Automated Security Solutions, Vulnerability Management, AI Ethics, Cybersecurity Policies.

1. Introduction

Today, digital technology is a big part of our economy. It's important to have strong cybersecurity to protect it. As we rely more on digital systems, cyber threats are also getting smarter. To tackle this, new rules like the **NIS2** Directive have been created. These rules help keep important services safe from cyber-attacks in the European Union. **NIS2** builds on the earlier **NIS** rules. It asks organizations to follow stricter security measures and manage risks better. Getting compliant with NIS2 can be tough, but new technologies can help. One of these is generative AI. It's a kind of smart technology that can help improve how we handle cybersecurity. Generative AI can automate boring tasks, help predict threats, and make security stronger. This means organizations can follow **NIS2** rules more easily. Plus, they can spot and fix risks before they turn into big problems. It also gives real-time insights, making it easier to stay safe with all the changing threats out there. In this piece, we'll look more closely at how generative AI can help with **NIS2** compliance. We'll share some examples and show how AI can improve processes like risk assessment and incident detection. As companies work to meet these rules and strengthen their cybersecurity, generative AI can be a great help. In the next sections, we will cover what generative AI can do, explain the specific **NIS2** requirements, and suggest ways to mix AI tools into existing cybersecurity efforts. By understanding how generative AI fits in, organizations can get ready to tackle both regulatory needs and new cyber threats.

1.1 Background of NIS2 Directive

The NIS2 Directive is all about boosting cybersecurity in the European Union. It builds on the original **NIS** Directive from **2016**. The goal is to tackle the growing digital threats that impact countries and the single market. The first **NIS** Directive focused on key services like energy, transport, banking, and healthcare. But as cyber threats got tougher, it was clear we needed a better plan. Here are some important reasons behind **NIS2**:

- *Cyber-attacks are happening more often and they're getting smarter. All probably heard of big cases like the SolarWinds hack or the Colonial Pipeline ransomware attack. These events showed us why we need better cybersecurity.*

- *As companies go digital, there are more ways for attackers to strike. This means we need to be tougher on security than ever before, pointing out where the current rules fall short.*

- *Cybersecurity isn't just a local issue. Hackers often work from different places. The NIS2 Directive is designed to help EU countries work together to deal with these problems.*

The **NIS2** Directive was proposed by the European Commission in **December 2020**. The European Parliament and the Council have since adopted it. The goal of this directive is to boost security with a few important rules.

- *The NIS2 Directive adds more types of organizations that need to follow its rules. It covers essential services like energy, transport, health, and digital systems. The main goal is to make sure more businesses follow better cybersecurity practices.*

- *The directive talks a lot about managing risks. It pushes organizations to put proper safety measures in place. They should take a risk-based approach to keep their systems safe.*

- *NIS2 also requires companies to report security incidents faster than before. They must tell the right authorities about big issues within 24 hours and submit a full report within a month.*

- *One big change in NIS2 is the attention to cybersecurity in supply chains. Companies need to manage risks that come from their third-party vendors.*

- *The directive wants countries in Europe to work together better. It sets up the European Cyber Crises Collaboration Framework to help with sharing important information and responding to crises together.*

- *NIS2 has tougher rules. There are big fines for organizations that don't comply. This is meant to push companies to take cybersecurity seriously.*

Once the EU member states adopt it, they need to turn the **NIS2** Directive into their own laws, usually within two years. This lets each country adjust the rules to fit their laws while still aiming for the same goals set by the EU. The **NIS2** Directive has made some key improvements compared to the old **NIS** Directive, which had a few issues.

- *The old rules focused mainly on essential services. But NIS2 expands this to cover more sectors. It knows that everything in the digital economy is connected.*

- *With NIS2, security needs to be stronger. This means better risk management and faster reporting of any incidents.*

- *The previous rules didn't really look at risks from third parties. But NIS2 makes it clear that companies must think about their supply chains when assessing risks.*

- *NIS2 emphasizes working together among EU countries. Cyber threats are a shared problem that everyone needs to tackle as a team.*

Some challenges to implementation are:

- *Groups might have a tough time following the new rules, especially small and medium-sized businesses. They usually don't have a lot of money or people for cybersecurity.*

- *Different countries might understand the rules in their own ways. This can create confusion and make things tricky for businesses working across borders.*

- *Putting in the right security measures could also cost a lot of money and need special skills. This might stretch some organizations thin.*

As the **NIS2** Directive rolls out, it's important to keep an eye on how well it's working and if it can adapt to new threats. We need both public and private sectors to keep talking and working together. Ongoing awareness and education are key to building a strong cybersecurity culture. Also, as technology changes, we'll need to update the directive to make sure it stays useful for future issues. The EU's focus on teamwork and new ideas will be a big

part of creating a strong digital economy.

1.2 Importance of Cybersecurity in Digital Transformation

The first **NIS** Directive came out in **2016**. It created rules for keeping online networks and information safe in the EU. Since then, cyber threats have gotten much tougher. We've seen big attacks and data breaches. Because of this, we needed stronger rules. That's why NIS2 was made. It builds on the first directive and covers more sectors and organizations. **NIS2** has important new rules to improve cybersecurity across the EU.

- *NIS2 affects medium and large companies in important areas. It sets out rules for essential service and digital service providers. This way, it helps keep more infrastructures safe.*
- *Companies must put strong risk management practices in place. This includes checking for risks and having plans ready for incidents.*
- *NIS2 also requires fast reporting of cyber incidents to the authorities. This helps make sure problems are dealt with quickly.*
- *Each Member State must assign a competent authority to check that companies follow NIS2.*
- *There is a bigger focus on supply chain security. This is because risks can spread through connected networks.*

Digital transformation is all about using digital tech in every part of a business. It changes how companies work and how they provide value to their customers. This includes things like cloud computing, AI, IoT, and data analytics. These tools can help companies run better and stay competitive. But with all these new tools comes a bigger chance of cyber risks. As companies switch to cloud services, use IoT devices, and analyze data, they open up more ways for hackers to attack. That's why strong cybersecurity is a must in digital transformation. It helps keep sensitive info safe and ensures that digital projects don't lead to problems.

Cyber-attacks can cost a lot. The global economy loses trillions every year to cybercrime when added up direct costs, recovery fees, legal bills, and damage to a company’s reputation. Small and medium businesses are often the worst hit since they often don't have the resources to fight off sophisticated attacks. By focusing on cybersecurity, businesses can protect their assets and keep running smoothly. **NIS2** is a rule meant to tackle the connected nature of digital spaces today. It includes important sectors like energy, transport, and healthcare. This rule understands that a weakness in one company can impact many others. While **NIS2** gives a strong plan to boost cybersecurity, businesses may face some challenges when putting it into action. These challenges include:

- *Lots of small and medium businesses have a tough time finding the right resources for compliance.*
- *It can also be hard to figure out all the rules if they don’t have a team just for that.*

- *Changing the company culture to care more about cybersecurity takes a lot of effort and planning.*

Technology is always changing. Here are some important trends that could influence the future of cybersecurity and **NIS2** compliance:

- *Cyber threats are getting tougher to handle. Because of this, many organizations are turning to AI and automation tools. These tools help spot threats more quickly and respond better.*

- *Instead of just reacting to attacks, companies are looking to be more proactive. They want to build stronger defenses all around.*

- *Businesses are teaming up to share information about threats. Working together like this helps everyone tackle cyber dangers better.*

1.3 Role of AI in Cybersecurity

The **primary objectives of NIS2** are to:

- ***Help** member states handle cyber threats better.*

- ***Boost** teamwork between member states and the EU.*

- ***Set** a higher standard for cybersecurity for key organizations.*

NIS2 covers important areas like energy, transport, health, and digital services. It puts new rules on both key and important organizations. This means some places that didn't think they needed to follow cybersecurity laws now have to. **NIS2** also brings in important new rules to boost cybersecurity.

- *Businesses need to have good risk management in place.*

- *They also have to report big cyber issues to national authorities quickly.*

- *Companies should think about the risks that come from their supply chains too. It's important for member states to work together better when responding to incidents and sharing information.*

AI's role in cybersecurity includes but is not limited to:

- *AI can look at network traffic and user actions to spot anything strange that might mean a cyber-threat.*

- *Machine learning can help speed up reactions to these threats so they get handled quickly.*

- *AI can also check malware faster than old methods, making it easier to deal with new problems.*

- *AI can scan emails and messages for phishing signs, which helps cut down on successful attacks.*

Integrating AI in cybersecurity offers several advantages:

- *AI can quickly handle lots of data. This helps spot dangers before they get serious.*
- *It can predict risks by looking at past data and trends.*
- *Automating simple tasks lets security experts concentrate on bigger issues.*

The **NIS2** Directive focuses on managing risks, reporting incidents, and working together between member states. This means we need fresh ideas to keep up with these demands. AI can really help organizations meet **NIS2's** goals. It can boost how well we spot threats for the businesses that need to follow **NIS2**.

- *AI systems can keep an eye on networks all the time.*
- *They can spot if there's an attack happening. If something weird goes on, these systems can send alerts to the IT team. This helps them act faster.*

In the context of **NIS2**, incident response protocols are vital. AI can support organizations in:

- *AI can react to threats quicker than humans. It can look back at incidents and explain how they happened.*
- *This helps find ways to prevent them in the future.*

Using AI in cybersecurity needs to follow the rules about data privacy, like GDPR in Europe. Companies must make sure they're using AI in ways that meet these legal standards. They also have to keep updating their security practices to stay in line with **NIS2**, which is changing often. AI helps by quickly spotting and reacting to new threats, which is key for staying compliant. **NIS2** also focuses on teamwork among countries. This helps with sharing information. AI can collect data from across the EU to spot trends in cyber threats. This can help everyone defend against attacks together.

1.4 Key Provisions and Requirements

The **NIS2** Directive, or Directive **(EU) 2022/387**, was created to improve how EU countries handle cybersecurity. It was made after seeing more cyber incidents and understanding the growing threats. Here are some of its main goals:

- *NIS2 wants to up our cybersecurity game in the EU. It aims to set a higher standard for network and information systems.*
- *The goal is to make sure key sectors can handle cyber threats. This keeps services running smoothly and protects people.*
- *NIS2 wants to make cybersecurity rules and reporting the same across all member states. This way, everyone can work together better on cybersecurity.*

The directive applies to **two** main categories of entities:

- *There are companies that offer important services we all rely on. This includes energy, transportation, banking, health care, and digital services.*

- *There are other sectors that matter too. They're not always seen as essential, but they still play a big role, think of manufacturing, food supply, and postal services.*

The **NIS2** Directive applies to:

- *All EU countries and the EEA countries are included.*
- *If a company is based outside the EU but works in any EU country, they may still need to follow these rules if they offer services there.*

Getting to know the terms in **NIS2** is important to really understand what it's all about. Here are some key definitions:

- *Things that can mess with the security of a network or information system.*
- *Any situation that could hurt the safety of an information system.*
- *A flaw in a system that bad actors can take advantage of to do damage.*
- *The steps to find, evaluate, and rank risks. Then we try to reduce, watch, and manage the chances or effects of unexpected problems.*

NIS2 is all about improving cybersecurity for important organizations. It lays out clear rules for managing risks, reporting incidents, and working together with other countries. A key part of NIS2 is that these organizations need to use good risk management and security practices.

- Companies should regularly check for risks. It's a good idea to do this at least every two years. Update it sooner if there are big changes.
- They also need solid security policies based on their risks and how it might affect their services.
- Companies should have basic technical and organizational steps in place. These steps can include:
  - *Control who can access what.*
  - *Keep the network safe.*
  - *Spot problems quickly and respond.*
  - *Train staff on security.*
  - *Have a plan for keeping the business running after a disaster.*
- *NIS2 focuses on keeping supply chains safe. It asks companies to check the cybersecurity risks that come from their third-party suppliers.*

NIS2 requires companies to report big incidents to the right authorities. This is a tougher rule than before.

- *If there's an incident that might interrupt vital services, organizations need to let the right authorities know within 24 hours.*

- *They should explain how serious the incident is and what it could mean for services.*
- *After the first report, they must send follow-up updates. These should include a thorough look at what happened, why it happened, and what steps they are taking to fix the issue.*

NIS2 is all about improving security in the EU. It stresses how important it is for countries and businesses to work together and share information.

- *NIS2 wants to set up joint cyber units. This will help national authorities work better together and team up with businesses.*
- *The plan also suggests creating platforms for sharing information about cyber threats, weaknesses, and incidents.*
- *It aims to improve cooperation between countries. This means they can act quickly when issues affect more than one-member state.*

Every country needs to pick a national authority to handle NIS2. This authority will watch over the cybersecurity of key businesses in its area. They will check these businesses regularly to see if they are following the rules of **NIS2**. These checks might include:

- *Check security audits.*
- *Look over incident response plans.*
- *Check how manage risks.*

NIS2 sets up rules for penalties if organizations don't follow the rules. Here are some possible penalties:

- *Fines for breaking the rules.*
- *Limits on how much they can operate.*
- *Public disclosures regarding non-compliance*

2. Impact on Organizations and Industries

Organizations that are part of **NIS2** need to put in place the right security measures. This includes things like:

- *Check for risks and make plans to handle them.*
- *Have a plan for spotting problems and fixing them.*
- *Review the safety of the supply chain.*
- *Train employees to be aware of security issues.*
- *Conduct regular security checks to find any weak spots.*

To meet these requirements, need to really understand your organization's digital assets and any weaknesses they may have. Also need to think about how cyber incidents could affect.

Reporting incidents quickly is key under the **NIS2** framework. Companies must set up ways to report any issues that might disrupt services. This means any serious problems that could affect their operations or put sensitive information at risk. The need for fast and thorough reporting puts a lot of pressure on organizations. They have to improve how they detect and respond to incidents. Following **NIS2** also means spending a lot on cybersecurity tools and practices. Companies will need to put resources toward:

- *Updating our security tech.*
- *Bringing in new security rules.*
- *Holding regular training for staff.*
- *Working with cybersecurity experts.*

Investing in cybersecurity can cost a lot, especially for medium-sized businesses. But not dealing with it could be even worse. The fines for not following the **NIS2** rules can hit up to **€10 million** or **2%** of global sales, whichever is more. That's a big push for companies to take cybersecurity seriously. To keep safe, businesses need to set up a strong risk management plan. This means they should figure out what systems are important, know what threats they might face, and create plans to keep services running smoothly. **NIS2** highlights that supply chain security is vital. Companies should check that their partners follow good cybersecurity practices too. This way, they can reduce risks and stay strong.

In today's world, people worry more about their data safety and service reliability. By sticking to **NIS2** and showing they care about cybersecurity, businesses can boost their reputation. This can lead to more loyal customers and a bigger market share. Following **NIS2** can be tricky, especially for companies with old systems that can't easily adapt. They might need to spend a lot of time and money to upgrade. Plus, finding skilled workers in cybersecurity is tough. Training current employees might be needed to fill that gap. For bigger companies that work across different EU countries, dealing with different rules and interpretations of **NIS2** can be a challenge. Creating a solid cybersecurity plan that meets all local rules and fits global standards will need teamwork and effort. With cyber threats always changing, companies must stay ahead. This means spotting potential dangers, checking their systems regularly, and updating their security as needed. They can also use new tech like AI and machine learning to boost their defenses. Investing in these tools can help them detect threats better and respond faster. To really meet the **NIS2** rules and strengthen their defenses, businesses need to make cybersecurity part of their culture. This means ongoing training, talking openly about risks, and encouraging everyone to be part of the solution.

2.1 Challenges in Achieving Compliance

NIS2 focuses on risk management and supply chain safety. Organizations need to use security measures based on the risks they face. They also have to report significant incidents to national authorities within a certain time. One big challenge is understanding what the directive really requires. It covers many sectors and has specific rules on what security measures to take. This can be confusing, making it hard for organizations to comply. Many

smaller companies might not know much about **NIS2** or what it means for them. Training and awareness programs can help, but often these programs don't get enough funding or attention. Some organizations may already follow different cybersecurity standards that don't match up with **NIS2**. This can lead to even more confusion and extra costs as they try to adjust their policies to meet the new requirements.

Following the strict rules of **NIS2** can cost a lot, especially for small to medium businesses. They need to spend on cybersecurity tools, training their staff, and keeping up with the rules. For many, money is tight and this can make it hard to meet those requirements. There's also a big shortage of skilled workers in cybersecurity. It's tough for companies to find and keep people who can set up the right security. This often leads to teams being overworked and security systems not working well. This increases the chance of falling out of compliance. Technology changes fast. This means companies have to keep updating their security to deal with new threats. The rules need to be flexible, but many businesses find it hard to keep up, which can lead to problems. Communication between IT security teams and management can often break down. When there's a messy process for spotting and reporting issues, companies can miss important things. This can lead to non-compliance and harm their reputation.

Supply chains today are complicated, and it's hard for companies to check if their suppliers are meeting NIS2 requirements. If one supplier has a problem, it can put all the others at risk, making compliance tough. Although **NIS2** wants to create some uniformity, different countries may understand the rules differently. This can confuse businesses that operate in several places and complicate compliance. Working with various national regulators can also be tricky, especially if there's no clear guidance. Companies should focus on training their workers to understand **NIS2** and their roles in compliance. A knowledgeable team helps build a culture of responsibility around cybersecurity. Regularly checking suppliers' security practices is key to following **NIS2** rules. Taking a risk-based approach to assess supplier risks is smart. Building good relationships with cybersecurity authorities and industry groups can help share knowledge and make compliance easier. Collaborating can improve understanding and lighten the load of compliance.

2.2 Different Types of AI Technologies Used

Artificial Intelligence, or AI, can look at big sets of data, find patterns, and learn from what it sees. This makes it super important in many areas, like cybersecurity. AI can boost regular security measures and provide new ways to tackle cyber threats. There are different types of AI, and they each have specific uses in cybersecurity.

- *Machine Learning (ML).*
  - *Machine learning algorithms can look at a lot of data to find harmful software using patterns we've seen before.*
  - *It can improve intrusion detection systems by learning from network traffic. This helps spot unusual activities that might mean an attack is happening.*
- *Natural Language Processing (NLP).*

- *NLP algorithms can look at messy data from places like forums, news articles, and reports. they help find important information about new threats.*
- *NLP is useful for spotting phishing attempts in emails. It does this by checking the words and context used in the messages.*

- *Computer Vision.*
  - *AI cameras with smart vision can spot when someone enters a restricted area. They can quickly notify security staff.*
  - *Looking at footage from security cameras helps find possible security threats.*
- *Anomaly Detection.*
  - *Spotting strange increases in traffic can help us check for DDoS attacks.*
  - *Keep an eye on how users act to find any signs of account hacks or insider threats.*
- *Predictive Analytics.*
  - *Look at old data to guess what cyber threats might come next. Then, get ready with some preventive steps.*
  - *Spot weaknesses in systems by checking out how past attacks worked.*
- *Automated Response Systems.*
  - *When a threat is spotted, the system can quickly shut off affected machines or stop harmful processes.*
  - *It can look for weak spots and flaws in systems before anyone takes advantage of them.*
- *Chatbots and Virtual Assistants.*
  - *Chatbots can help users with questions about cybersecurity. They can share tips on how to stay safe online.*
  - *Virtual assistants can make it easier to report problems. They help companies keep track of incidents and respond quickly.*

Organizations can use AI to catch threats in real time. By combining machine learning with network monitoring, they can spot potential risks before they happen. AI helps make handling incidents faster and easier. It can automatically find, contain, and fix cyber threats. This matches up with **NIS2's** need for quick reporting and action. With AI, organizations can predict risks better. They can check for weak spots and guess where threats might come from. This helps them make smarter choices about managing risks. AI also makes it easier for groups and government bodies to share information. Automated systems can send out updates on threats. This keeps everyone in the loop about new risks and how to respond together. But using AI isn't all smooth sailing. Organizations face some challenges, like:

- *Gathering and analyzing a lot of data can raise privacy issues. It's important to follow data protection laws.*

- *Sometimes, machine learning can pick up on biases. This can result in unfair practices when identifying threats or handling incidents.*

- *There aren't always enough skilled workers in AI and cybersecurity. This makes it hard for organizations to use these technologies well.*

2.3 Limitations and Risks of AI in Cybersecurity

AI needs good data to learn well. But sometimes, companies don't have enough data, or their data is not right. When the data is poor, AI models don't work as they should. Many AI models, especially deep learning ones, are hard to understand. This makes it tough for cybersecurity experts to trust their outputs. Even with smart AI, we still need people to oversee the systems. Cybersecurity professionals have to keep an eye on AI tools. They need to check how well they're doing and make changes when needed. AI isn't perfect. It can sometimes wrongly flag safe actions as threats or miss actual threats. These mistakes can cause security issues or waste resources chasing false alarms. AI can also have biases from the data it learns from. This can lead to unfair treatment of different users or situations. It raises concerns about fairness and accountability in how AI makes decisions, especially in sensitive areas like cybersecurity. AI can help companies meet **NIS2** rules by automating reports, checking for weaknesses, and improving security measures. However, companies need to plan how they'll use AI to work well within these guidelines. They might run into problems when trying to use AI for **NIS2** compliance. These problems could include:

- *Companies need to put money into both people and tech to get AI systems up and running.*

- *Following data protection rules might make it hard to use AI effectively in keeping data safe.*

- *Mixing AI with current systems in different setups can be tricky and might need big changes.*

2.4 Comparison with Traditional AI Techniques

Traditional AI uses different methods and algorithms to do tasks that usually need human smarts. Some examples are machine learning, natural language processing, and expert systems. AI finds its use in many areas like finance, healthcare, and cybersecurity. Here are some of the main traditional AI techniques:

- *Algorithms get better at tasks as they learn from experience. Some common methods are supervised learning, unsupervised learning, and reinforcement learning.*

- *There are methods that help machines make sense of human language. These are used in chatbots, understanding feelings in text, and sorting through information.*

- *Expert systems mimic how a human expert makes decisions. They use a knowledge*

base and rules to help them figure things out.

- *There are computer systems modeled after our brains. They can spot patterns and make guesses about what might happen next.*

Applications of traditional AI in Cybersecurity:

- *AI is used to spot weird stuff and possible threats in network traffic.*
- *It helps systems tell the difference between normal and suspicious activity.*
- *AI also helps analyze malware, which means we can react to threats faster.*
- *With AI, we can automatically respond to threats, cutting down the time it takes to handle attacks.*

Risk management is a key part of **NIS2**. Regular risk assessments can take a lot of time and may be based on personal views. AI can help make this process quicker by:

- *AI tools can look at past data to guess what might happen in the future. This helps in managing risks ahead of time.*
- *AI monitors network traffic and systems in real-time. This means it can check for risks constantly.*

NIS2 wants quick reporting of security incidents. So, it's really important to spot and deal with these problems fast. AI can help with this in a few ways:

- *AI can spot regular behavior and quickly notice when something's off.*
- *It can help create incident reports automatically, making sure they meet NIS2's deadline.*

NIS2 focuses a lot on keeping the supply chain safe. AI can help organizations check how well their suppliers handle cybersecurity. This includes:

- *AI can check how safe third-party vendors are. It helps companies see the risks involved.*
- *By using AI, businesses can keep an eye on their suppliers' cybersecurity. This way, they can make smarter choices.*

Traditional AI and AI solutions for NIS2 both aim to boost cybersecurity. They do this by using automation, being efficient, and predicting threats. Traditional AI mainly helps with spotting and responding to threats. On the other hand, NIS2-related solutions cover risk management and ensuring compliance with regulations. Traditional AI can be used in many ways, but NIS2-focused AI needs special features to meet legal requirements. Here are the main differences:

- NIS2 needs solutions that meet certain rules in the industry.
- *Regular AI tools usually apply to a wider range of tasks.*

- *NIS2 pushes for better teamwork among member states and organizations. This means AI tools have to help share information and work together.*

- *AI tools for compliance should be flexible so they can keep up with changing rules and standards.*

Traditional AI techniques are strong, but they have some limits. We need to address these when it comes to **NIS2** compliance.

- *A lot of classic AI methods use old data. This data can get old pretty fast as new cyber threats come up.*

- *Deep learning models often aren't very clear. It's tough to see how they make decisions. This is a big deal for following rules and regulations.*

- *Traditional AI systems often need a lot of human help. This can slow down how quickly we respond to incidents.*

As companies work to follow **NIS2** rules, we'll see some big changes in how they use AI to boost cybersecurity.

- *It's important to create AI systems that explain their decisions clearly. This will help meet rules and regulations.*

- *Working together, different organizations can train AI models while keeping data private. This teamwork can make spotting threats even better.*

- *We need AI that learns from new information all the time. This is key to staying ahead in the fast-changing world of cybersecurity.*

AI is doing a lot in cybersecurity. But we still need human skills. To follow **NIS2** rules well, we need both AI help and human thinking.

- *AI can help cybersecurity experts by giving them useful information. This helps them make better choices.*

- *Companies need to train their staff to use AI tools well. It's important they know how to understand the data that AI provides.*

2.5 Applications of Generative AI in Cybersecurity

Generative AI has come a long way thanks to better natural language processing and machine learning. New tools like Generative Adversarial Networks and transformers help create smart AI models that can make great content. Here are some main types of generative AI models:

- *Generative adversarial networks, or **GANs**, have two parts. One part makes content, while the other checks if it's good. They work together to get better at creating things.*

- *There are variational auto encoders, or **VAEs**. These are used when we don't have labeled data. VAEs can create new examples that are similar to what they were trained on.*

- *We have **transformers**. These models are popular for tasks involving language. They*

can create text that makes sense, based on what someone give them as a starting point.

Generative AI can help spot threats by looking at big sets of data. It finds patterns that show bad behavior. By learning from past attacks, AI can create profiles of possible risks. This lets companies act before problems start. AI tools can also handle security issues on their own. They use set responses and real-time info to tackle threats quickly. This speeds up how fast organizations can react and handle problems. When it comes to managing weaknesses, AI can act like an attacker. It simulates attacks to find spots that need fixing. This helps companies stay one step ahead of threats. With **NIS2** pushing for better reporting, AI can make this easier. It can automatically whip up reports using data and logs. This cuts down on paperwork and makes sure reports are on time. Generative AI can create realistic training for cybersecurity teams. It sets up fake attacks and phishing emails to train workers. This boosts their skills and keeps them ready for real threats.

NIS2 and generative AI are set to change how we handle cybersecurity. Companies are putting more focus on following rules and using AI can help boost security. But there are some bumps along the road. We need to think about data privacy, make sure we follow the laws, and find people with the right skills. Policymakers have a lot to think about when it comes to AI in cybersecurity. They need to create clear rules about how we use AI, what's right and wrong, and who's responsible. This will help keep our online spaces safe.

2.6 Potential Benefits for NIS2 Compliance

One big benefit of following **NIS2** rules is better cybersecurity for your organization. These rules require strong risk management practices. This can help to:

- *Organizations need to spend money on better cybersecurity tools and methods. This will help them defend against online threats.*
- *They have to do security checks often. This way, they can find and fix any weaknesses quickly.*

Cyber incidents can cause big money problems. Data breaches, service outages, and fines can really add up. Following **NIS2** rules can help companies reduce these risks by:

- *Better response plans really help cut down on downtime when there's a cyber problem. This means less money lost.*
- *Insurance companies often look at how well businesses protect themselves online. If they follow the NIS2 rules, might pay less for insurance. That's because they see them as a lower risk.*

Nowadays, people care a lot about data security. Showing that they follow **NIS2** rules can really boost your organization's good name. Here are some benefits:

- *People are more likely to trust businesses that show strong cybersecurity practices.*
- *Following the rules can help a company stand out and stay ahead of the competition.*

NIS2 says that companies need to make plans for handling incidents and do regular training.

This results in:

- *Good incident response techniques can help bounce back faster.*
- *Regular drills and checks keep everyone in shape. They help companies learn new ways to handle fresh threats.*

NIS2 highlights how important it is for EU countries to work together, especially when there's a big cyber issue. Here are some benefits of working together:

- *Countries can pool their resources and skills. This helps create a stronger defense together.*
- *Clear lines of communication make sure everyone hears about issues fast. That way, they can respond quickly.*

Following **NIS2** can build better relationships between public institutions and private companies.

- *Public and private companies can work together on training exercises. This helps everyone understand the threats and how to respond.*
- *They can share information about new threats and weaknesses.*

Investing in cybersecurity as required by **NIS2** can save money in the long run.

- *Strong cybersecurity helps stop expensive hacks. These breaches can cost companies millions.*
- *Better cybersecurity makes things run smoother. This can cut down on extra costs too.*

A strong digital system is key for encouraging new ideas.

- *Following the rules can help companies feel good about using new tech. It can lead to more creative ideas.*
- *When they keep their networks safe, they protect their important info. This helps them come up with even better solutions.*

NIS2 compliance brings a lot of benefits. It pushes organizations to rethink how they handle cybersecurity. They start to put money into better resources and focus on improving their security all the time. The main goal of **NIS2** isn't just to follow rules. It's about creating a safer digital space in Europe that helps everyone involved.

3. Identifying Compliance Gaps through AI

Artificial Intelligence AI plays a critical role in identifying compliance gaps and enhancing an organization's overall cybersecurity posture, especially when navigating complex regulatory frameworks like the **NIS2** Directive. Bella, Castiglione, and Santamaria (2024) outline an ontological approach that enables AI to interpret and model intricate articles and relationships within directives. This structured and interoperable context allows for automated reasoning to highlight inconsistencies and omissions in compliance, helping

organizations pinpoint areas requiring attention. Additionally, AI-driven natural language processing (**NLP**) can parse the complex language of directives and map them against organizational practices, facilitating more effective and proactive compliance management.

Building upon the significance of NLP in compliance management, Lai (2024) emphasizes its role in extracting constraints from the **NIS2** directive for compliance monitoring. NLP-based methods can process legal documents to identify key regulatory markers such as "**shall,**" "**should,**" and "**must**" which are essential for understanding compliance obligations. This method not only automates the identification of compliance requirements but also categorizes them into actionable domains, such as operational measures, incident reporting protocols, and information-sharing obligations. By automating these processes, organizations can enhance the efficiency of their compliance efforts, reduce manual intervention, and minimize the risk of overlooking critical details. Furthermore, to address the evolving nature of cyber threats and regulatory requirements, underscores the necessity of integrating AI-driven data analysis and risk assessment as essential tools for maintaining compliance with directives like **NIS2**. His research demonstrates that proactive, AI-based strategies not only facilitate the identification of compliance gaps but also enhance an organization's capacity to adapt to shifting regulatory landscapes and emerging cyber threats. By utilizing comprehensive data analysis, organizations can better anticipate vulnerabilities and align their security frameworks with NIS2's stipulations, supporting robust incident response and fostering cross-border collaboration among member states. Integrating AI into compliance processes enables entities to remain resilient and compliant in a rapidly changing cybersecurity environment.

3.1 AI-driven Risk Assessment and Management

While the **NIS2** directive does not explicitly mandate the use of artificial intelligence AI, it strongly encourages the adoption of innovative technologies, including AI, to enhance cybersecurity measures. As organizations increasingly incorporate artificial intelligence (AI) in their operations, the need for comprehensive risk assessment and management becomes crucial. Ricciardi Celsi (2023) proposes a structured approach that combines the Data Benefit Index (DBI) and the SAFE framework to evaluate the risk profile and potential value of AI projects. This dual approach underscores the relationship between the risk levels associated with AI systems and their generated value. Specifically, the SAFE framework measures key aspects such as sustainability, accuracy, fairness, and explainability, aligning AI deployment with compliance obligations set by the AI Act. The combination of these frameworks aids organizations in balancing innovation and regulatory adherence by optimizing the benefits of AI while managing inherent risks.

Building on Celsi's framework for risk-aware AI governance, it is crucial to consider the regulatory expectations detailed in the **NIS2** Directive. Schmitz-Berndt (2023) emphasizes that the Directive's expansion of reporting obligations to incidents capable of causing significant operational disruptions or financial losses reflects an evolved understanding of cybersecurity risk. This change underscores the importance of incorporating "**potential harm**" into risk assessments. By leveraging AI-driven analysis tools, organizations can

identify vulnerabilities that, even if mitigated or contained, must be reported to contribute to a complete threat landscape. This proactive reporting helps not only in regulatory compliance but also in enhancing sector-wide intelligence and resilience.

Such an approach aligns with the directive's goal to prepare entities for emerging and evolving threats. Schmitz-Berndt highlights that recognizing and acting upon potential harm facilitates a comprehensive threat response strategy, encouraging the use of AI technologies for real-time monitoring and adaptive security measures. By employing AI to evaluate these aspects, organizations can effectively meet the directive's requirements and foster an environment of continuous risk assessment and improvement.

3.2 Automation of Compliance Processes

The **NIS2** Directive and automation of compliance processes with AI tools are two important developments in the field of cybersecurity and regulatory compliance. Let's explore how they intersect and how AI can help organizations meet **NIS2** requirements. AI technology can significantly streamline compliance and governance tasks by automating repetitive and time-consuming processes. Patel (2023) discusses how AI-driven systems can collect and correlate information, identify behavioral patterns indicative of compliance issues, and extract relevant entities from documentation. This capability enhances the monitoring of financial and operational records, detects anomalies, and even forecasts potential non-compliance incidents. The automated nature of these tasks helps reduce the human resource burden associated with traditional compliance checks, leading to faster, more accurate, and more cost-effective compliance management. By integrating AI into compliance frameworks, organizations can ensure consistent adherence to regulatory standards, minimize human errors, and maintain updated compliance protocols across their operations. Ekuma (2023) highlights that the integration of AI and automation can lead to enhanced efficiency and personalization in regulatory tasks. By harnessing machine learning and predictive analytics, organizations can adapt compliance processes to anticipate and address regulatory changes dynamically. This adaptability ensures that compliance strategies remain responsive to evolving frameworks like the NIS 2 Directive. AI tools also provide real-time data analysis, which enables more informed decision-making and proactive risk management. The ability of AI to process vast datasets quickly allows compliance teams to focus on strategic tasks rather than manual data management, thus enhancing the overall effectiveness of compliance programs. The automation of these processes not only ensures consistency and reduces human error but also fosters a culture of continuous improvement, where compliance protocols can be updated and refined based on emerging trends and insights.

In conclusion, the integration of AI into compliance processes offers significant benefits, aligning with the **NIS2** Directive's goals of enhancing cybersecurity and regulatory adherence. Through automation, organizations can reduce the burden of manual compliance tasks, improve accuracy, and respond more effectively to evolving regulatory requirements. By leveraging predictive analytics and real-time data analysis, compliance strategies become more dynamic and proactive, ensuring continuous alignment with best practices and

regulatory changes. This automated approach fosters a more resilient and efficient compliance framework, positioning organizations to navigate the complex landscape of modern cybersecurity regulations with greater confidence and efficiency.

4. Data Privacy and Protection under NIS2

The **NIS2** Directive significantly enhances data privacy and protection by embedding robust cybersecurity measures as foundational requirements for organizations. Schmitz-Berndt (2023) emphasizes the critical interplay between incident reporting under the **NIS2** Directive and data breach obligations under the GDPR. While GDPR focuses on protecting personal data, **NIS2** broadens its scope to ensure the security and integrity of the entire network and information system infrastructure. This dual approach not only safeguards individual rights but also reinforces overall system reliability, addressing vulnerabilities that could lead to significant data breaches. The directive further mandates proactive measures, such as reporting incidents capable of causing substantial harm, to build a comprehensive threat landscape, thus strengthening organizational preparedness and resilience.

4.1 Ethical Implications of AI in Cybersecurity

Generative AI tools, such as ChatGPT, have introduced significant ethical challenges in the realm of cybersecurity. Gupta et al. (2023) highlight the dual-use nature of these tools, where their capabilities can be exploited for both defensive and offensive purposes. On the defensive side, AI aids in enhancing threat intelligence, automating incident response, and fostering secure coding practices. However, the same tools are vulnerable to misuse, enabling malicious actors to bypass ethical constraints, craft sophisticated social engineering attacks, or generate malicious code. This misuse raises concerns about accountability and the ethical boundaries of AI deployment in cybersecurity contexts. Moreover, the authors emphasize that the inherent biases within AI models, stemming from their training data, can perpetuate harmful stereotypes or reinforce systemic inequalities. These biases, coupled with potential misuse scenarios, underscore the necessity for robust ethical guidelines and continuous monitoring of AI's deployment in cybersecurity. The development of secure, transparent, and bias-aware AI systems is essential to mitigate these ethical risks while maximizing the potential benefits of AI in enhancing cybersecurity frameworks.

4.2 Innovations in Generative AI for Cybersecurity

Generative AI **(GAI)** has become a transformative force in cybersecurity, introducing innovative capabilities to address the evolving threat landscape. According to Sai et al. (2024), GAI technologies such as ChatGPT, DALL-E, and other advanced generative models are being integrated into cybersecurity systems to enhance their robustness and adaptability. These models empower organizations to detect advanced phishing attacks, simulate attack scenarios, and automatically respond to threats with greater accuracy and efficiency. One key innovation lies in the ability of GAI to generate simulated environments, known as cyber ranges, where security professionals can test their systems and train for real-world threats. Additionally, GAI facilitates advanced threat intelligence by analyzing vast datasets, identifying patterns, and predicting potential attack vectors. This enables proactive defense

strategies that keep organizations ahead of malicious actors. Tools like Google Cloud Security AI Workbench and SentinelOne Purple AI leverage GAI to offer cutting-edge solutions for malware detection, phishing resilience training, and network anomaly identification.

5. Conclusion

Generative AI is changing the game for cybersecurity, especially when it comes to following the EU's **NIS2** rules. These rules aim to boost cybersecurity across Europe. They focus on managing risks, reporting incidents, and protecting important systems. With the growing number of cyber threats, generative AI can really help. It allows organizations to spot threats in real-time. This means they can find and fix problems before they become serious. By using machine learning, these systems can sift through loads of data to see patterns that might indicate a cyber-attack. Generative AI can take care of routine tasks. This gives cybersecurity teams more time to focus on important strategy work, helping to use their resources better and strengthen their overall security.

Reporting incidents is another big part of NIS2. Generative AI can make this easier by automatically creating reports. This helps organizations meet legal needs and keeps communication clear with everyone involved. It builds trust and accountability. Generative AI also helps improve cybersecurity methods. It can simulate cyber-attacks so organizations can test their defenses. These tests help refine security efforts and prepare for future threats. Using generative AI has its challenges. Organizations must be careful to follow ethical guidelines. They need to ensure that their AI tools don’t create new problems or biases. There should be good training and oversight to keep everything fair and transparent. As companies rely more on AI, they also need to be on guard against attacks aimed at AI systems. This means they have to think about securing both AI and traditional security practices together.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Canadian Center of Science and Education.

The journal and publisher adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.

Open access

Copyrights

References

Bella, G., Castiglione, G., & Santamaria, D. F. (2024). An ontological approach to compliance verification of the NIS 2 directive. Preprint retrieved from Department of Mathematics and Computer Science, University of Catania.

Bertino, E., & Islam, I. N. (2022). AI and machine learning for cybersecurity: A comprehensive review. *Security and Privacy*.

Ekuma, K. (2023). Artificial intelligence and automation in human resource development: A systematic review. *Human Resource Development Review*.

ENISA (European Union Agency for Cybersecurity). (n.d.). EU cybersecurity index. Retrieved from https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/eu-cybersecurity-index

ENISA (European Union Agency for Cybersecurity). (n.d.). NIS Directive - New version. Retrieved from https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

Galvão, R. J. V. (2024). NIS2 directive analysis and preparation for its implementation. Master's thesis, Faculty of Sciences and Technology, University of Coimbra.

Ghaffari, A., & Al Marashdeh, I. (2023). Generative AI in cybersecurity: Opportunities and challenges. *Computer Security Journal*.

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy.

Lai, H. C. F. (2024). Optimizing the IT auditing process: A business process redesign aligned with the NIS2 directive. Master's thesis, Eindhoven University of Technology.

Patel, D. (2023). Streamlining compliance and governance with AI in cloud-based programs. *International Journal for Multidisciplinary Research*, *5*(4), 1-11.

Ricciardi Celsi, L. (2023). The dilemma of rapid AI advancements: Striking a balance between innovation and regulation by pursuing risk-aware value creation. *Information*, *14*(12), 645. https://doi.org/10.3390/info14120645

Sai, S., Yashvardhan, U., Chamola, V., & Sikdar, B. (2024). Generative AI for cybersecurity: Analyzing the potential of ChatGPT, DALL-E, and other models for enhancing the security space.

Schmitz-Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*, *9*(1), tyad009. https://doi.org/10.1093/jcs/tyad009

Vijayakumar, V., & Manikandan, M. (2023). Assessing the impact of generative AI on cybersecurity practices. *International Journal of Information Security*.