Evaluation of Anti-Abuse Strategies Among Hosting Providers

A data-driven analysis of malicious IPs and compliance practices

by

Meixuan Niu

Student Name	Student Number
Meixuan Niu	4589858

Instructor:	Dr.ir.C.Hernandez Ganan
	Pro.dr.ir.P.H.A.J.M.van Gelder
	Dr.ir.M.Tuler de Oliveira
Project Duration:	Sept, 2024 - Jan, 2025
Faculty:	Technology, Policy and Management, Delft

Style: TU Delft Report Style, with modifications by Daan Zwaneveld

TU Delft

Abstract

Hosting providers are essential for maintaining the security and reliability of digital services, but they continue to face challenges from malicious activities in their network, such as malware and phishing. The European Union's Digital Services Act (DSA) was introduced to improve accountability and create a safer online environment, but its effectiveness in helping hosting providers mitigate abuse remains unclear. This study investigates whether compliance with the DSA has contributed to reducing malicious activity among Dutch hosting providers and examines the broader relationship between compliance levels and cybersecurity outcomes.

This study evaluates the effectiveness of anti-abuse measures employed by Dutch hosting providers, with a focus on the role of the DSA in helping with compliance and reducing malicious activity. Specifically, it examines whether adherence to the DSA improves the ability of hosting providers to mitigate cyber threats, particularly in reducing the prevalence of malicious IP addresses. Using passive DNS data, the research examines changes in the prevalence of malicious IP addresses before and after the implementation of the DSA. Compliance levels were also analyzed to understand their correlation with malware percentages. The study employed statistical methods, including Interrupted Time Series (ITS) analysis and regression models, to evaluate trends and relationships between compliance and malicious activity.

The findings indicate no statistically significant reduction in malicious IP activity following the implementation of the DSA, suggesting that compliance alone does not automatically translate into improved security outcomes. While the DSA strengthens transparency and procedural accountability, hosting providers continue to face operational challenges in implementing effective anti-abuse measures. Factors such as cybercriminal adaptation, enforcement inconsistencies, and resource constraints likely influence the weak correlation between compliance and actual abuse reduction. These results shows the need for a more holistic approach to cybersecurity regulation, combining technical advancements, industry collaboration, and proactive security enforcement alongside regulatory compliance. Evaluating the effectiveness of frameworks like the DSA is essential to ensuring that they not only establish compliance standards but also provide hosting providers with practical tools to enhance online security and mitigate digital threats effectively.

Contents

1

Introduction

1.1. Background

Hosting providers facilitate the operation of websites, applications, and other essential online tools, making their services indispensable to businesses and individuals. However, hosting providers face increasing threats from malicious actors who exploit their networks for malicious activities such as malware distribution, phishing, and botnet operations. These threats undermine trust in digital services and highlight the need for anti-abuse strategies and measures.

Even hosting providers might already employed various security measures, the the sophistication of cyber threats continues to grow, requiring advanced detection methods and proactive measures to mitigate risks effectively.

Regulations like the European Union's Digital Services Act (DSA) place greater responsibilities on hosting providers, requiring them to meet stricter standards for compliance and accountability. In the Netherlands, which has a rather advanced digital infrastructure, hosting providers play a key role in keeping the online environment secure and reliable. Their ability to implement effective anti-abuse practices is essential for maintaining the safety and integrity of the country's digital ecosystem. At the same time, these providers face the challenge of complying with regulatory requirements while dealing with cyber threats. This study focuses on evaluating the impact of the Digital Services Act (DSA) on the anti-abuse measures employed by hosting providers, particularly in the Netherlands, and whether these measures have been effective in reducing malicious activities.

1.2. Research Problem

Hosting providers play an important role in keeping digital services secure and functional. However, they face growing challenges in dealing with abuse within their networks, including threats like malware, phishing, and botnet attacks. Even though many providers have implemented anti-abuse measures, there is little research examining how effective these practices are with real data of abuse.

New regulatory requirements that are aimed to help hosting providers in combating abuse activities in their networks can also pose challenges to them, such as the European Union's Digital Services

Act (DSA). The DSA places new responsibilities on hosting providers, but it is unclear how well these regulations are helping providers improve their ability to mitigate abuse. There is also a limited exploration of how real historical data, like passive DNS records, can be used to evaluate whether these regulations are making a difference.

Another issue is that hosting providers face different challenges depending on their size and resources. Smaller providers may lack the tools or expertise needed to comply with regulations, while larger ones often deal with scale-related issues. These differences make it harder to understand how regulations like the DSA affect providers in practice. Without further research, it remains challenging to create effective strategies that help hosting providers comply with regulations while addressing the increasing demands for stronger security measures.

1.3. Research Objectives and Questions

The primary objective of this research is to investigate the impact of the Digital Services Act (DSA) on the effectiveness of anti-abuse measures employed by Dutch hosting providers and to identify the challenges they face in mitigating abuse. This study aims to evaluate changes in the prevalence of malicious IP addresses associated with Dutch hosting providers before and after the implementation of the DSA, providing a quantitative assessment of its impact. Additionally, the research seeks to examine how compliance with DSA requirements correlates with the percentage of malware observed within hosting networks. It also explores the specific anti-abuse measures currently in use by hosting providers and evaluates their effectiveness in detecting and mitigating malicious activity. Another focus is to clarify the requirements imposed by the DSA on hosting providers when implementing these measures. Finally, the study aims to analyze how factors such as hosting provider size and operational focus (e.g., public-facing versus enterprise-focused) influence their ability to meet DSA obligations and address malware effectively.

1.3.1. Research question

How has the implementation of the Digital Services Act (DSA) impacted the effectiveness of anti-abuse measures employed by Dutch hosting providers, and what requirements do they face in mitigating abuse?

1.3.2. Sub-questions

- What is the percentage of malicious IP addresses associated with Dutch hosting providers, and how has this changed before and after the implementation of the DSA?
  - How should hosting providers be defined in the context of this research?
  - What is considered as malicious IP?
- How do compliance levels with the Digital Services Act (DSA) requirements correlate with the malware percentages of Dutch hosting providers?
- What anti-abuse measures are currently employed by these hosting providers to detect and mitigate malicious activity?
- What requirements according to the DSA do hosting providers need to meet when implementing effective anti-abuse measures?
- How do hosting provider size and focus (e.g., public-facing vs. enterprise-focused) influence their compliance with DSA obligations and malware rates?

2

Literature review and theoretical background

2.1. Introduction to cybersecurity in hosting environments

Hosting services are integral to the internet's infrastructure, providing platforms for websites, applications, and online services. However, they are also frequently exploited for malicious activities, including malware distribution, phishing, etc. Recent data underscores the severity of this issue:

Globally, the impact of cyber threats has become more severe than before. According to the World Economic Forum's 2023 Global Cybersecurity Outlook, 91% of surveyed business and cybersecurity leaders expressed concerns that geopolitical instability could trigger a widespread cyber event in the next two years. Such events have the potential to disrupt not only digital infrastructure but also critical systems worldwide (Forum, 2023).

Among all cyber threats, malware remains to be a critical concern due to its scale and impact. According to Statista, the number of malware attacks worldwide has been substantial, with billions of incidents reported annually (Statista, 2023). This data shows the ongoing challenges that hosting providers face in mitigating malware threats and the necessity for robust security measures to protect hosted services and their users.

Emerging threats make the mitigation of these risks more complicated. Cybercriminals are now using technologies like public cloud services to generate millions of hidden malicious URLs. These URLs allow phishing and malware attacks to scale up massively, making them harder to detect and more dangerous (Kazim & Evans, 2016).

These challenges highlight the critical role that web hosting providers play in either facilitating or combating cyber threats. The concentration of malicious activities within specific hosting networks emphasizes the need for robust cybersecurity measures and vigilant monitoring to protect users and maintain the integrity of online services.

2.1.1. Importance of cybersecurity for hosting providers

(von Solms & van Niekerk, 2013) mentioned that, in the past, cyber security is more about protecting information and keeping data from unauthorized access. However, this paper pointed out, the concept of security is more than protecting information assets, it involves securing the critical infrastructure such as, servers, networks, and other essential components that our digital environment depends on. For hosting providers, this means it is important to adopt a more comprehensive approach to security that addresses the potential threats, from data breaches to infrastructure attacks.

This shift is especially important in the context of cloud computing. As (Kshetri, 2010) notes, cloud computing offers many advantages, such as cost savings and access to advanced IT resources. However, it also introduces new security challenges. In a cloud environment, data is often shared across multiple locations worldwide, making it more difficult to protect. When a hosting provider needs to manage a complex environment like that, it must ensure that not only is the data secure, but the entire infrastructure is protected from potential cyberattacks. In his article, Kshetri emphasizes the importance of safeguarding information in cloud computing, due to the global economy's reliance on cloud-based services, such as Salesforce and other essential software.

Moreover, (Mueller, 2010) mentioned in his book, hosting providers also play a role in setting cybersecurity standards since they often operate in a complex global landscape where various stakeholders, including governments, private companies, and international organizations, (Mueller, 2010) emphasizes the importance of global governance, where these stakeholders collaborate to manage and secure the internet. Hosting providers need to follow international rules and collaborate with other organizations to protect their networks. It is crucial for countries and companies to work together to stay safe because cyber threats can spread quickly from one part of the world to another. (Mueller, 2010).

According to (Eeten et al., 2010), an important part of the hosting providers' responsibility is to detect and prevent potential cyberthreats, he particularly mentioned the challenges posed by botnets. (Eeten et al., 2010)argues that hosting providers are in a uniquely advantageous position to address these threats because they manage the essential infrastructure that botnets frequently exploit to launch their attacks.

To successfully detect and mitigate the risks posed by botnets, hosting providers can adopt a proactive approach. This involves the continuous monitoring of network traffic to identify any unusual patterns or activities that show the potential presence of a botnet (Eeten et al., 2010). Other than monitoring network activities, collaborating with other organizations and sharing information about new and emerging threats can help these organizations enhance their ability to identify and counteract potential attacks before they escalate(Eeten et al., 2010).

2.2. Overview of cyber threats in hosting environments

2.2.1. Type of cyber threats

Malware

Hosting providers face many types of threats that require well-designed security measures for effective detection and mitigation. According to (Hernandez-Suarez et al., 2022), malware is one of the most common threats, with ransomware and cryptojacking being explicitly discussed. It means that the computer resources are maliciously exploited and used to mine cryptocurrencies without the user knowing and allowing it. It is challenging to detect because it operates quietly in the background, maliciously

exploiting computer resources to mine cryptocurrencies without the user's knowledge. This type of attack can remain undetected for a long time, costing resources and influencing server performance negatively. Thus, (Hernandez-Suarez et al., 2022)emphasize it is important to employ advanced detection methods, such as machine learning, which can analyze patterns and behaviors associated with malware, making it possible to identify attacks that traditional methods might miss.

There are other advanced method used by attackers other than this type of Malware. For instance, (Antonakakis et al., 2011) discussed how Domain Generation Algorithms (DGAs) are employed to create numerous domain names for distributing malware and maintaining command-and-control (C&C) infrastructure. These algorithms can generate many domain names quickly, making it difficult for traditional security systems to block them all. The Kopis system, as introduced by (Antonakakis et al., 2011), utilizes passive DNS data to detect these malicious domains at the higher levels of the DNS hierarchy, such as top-level domains (TLDs). By monitoring DNS traffic patterns, Kopis can identify and block domains associated with malware, often before they appear on public blacklists, thereby enhancing the effectiveness of malware detection beyond traditional measures.

Phishing

(Jyothi et al., 2024)emphasized that phishing is another security threat. Phishing involves tricking individuals into revealing sensitive information, such as passwords or credit card information, by pretending to be a legitimate entity. Attackers often use emails or illegitimate URLs to trick victims into providing this information. Once the attackers have the information, they can use it for fraudulent activities, such as stealing money or accessing sensitive accounts.

In the research conducted by (Jyothi et al., 2024), machine learning models have demonstrated significant effectiveness in detecting phishing attacks, such as by recognizing email content and website characteristics. However, implementing these models in real-world applications presents several challenges. For instance, machine learning models require large datasets to train effectively, which requires a lot of data collection and preprocessing efforts. Maintaining and improving these algorithms can also be costly.

(Bilge et al., 2014) further explored how passive DNS data can be used to identify phishing domains before they become widely recognized as threats. Their system analyzes DNS query patterns, such as how often a domain is queried and from where, to detect domains that are likely being used for phishing. For example, a domain that suddenly receives a large number of queries from different parts of the world might be flagged as suspicious. This early detection capability allows hosting providers to block phishing domains before they can cause significant harm.

DDoS attacks

DDoS attack is another type of threat that is mentioned and significant to hosting providers. In a DDoS attack, the targeted server gets flooded by a large number of compromised computers. The server will be overwhelmed and lose availability to users. It can lead to downtimes, and while not properly managed, it can disrupt the business.

To mitigate this risk, (Hyder et al., 2022) discussed the use of moving target defense (MTD) mechanisms in cloud hosting environments to protect against DDoS attacks. MTD works by constantly changing the attack surface, such as by altering IP addresses or shifting server locations, making it more difficult for attackers to target the server effectively. This strategy increases the complexity and cost for attackers, forcing them to expend more resources to carry out the attack. For hosting providers, implementing

MTD can be an effective way to reduce the risk of successful DDoS attacks and maintain service availability.

Another interesting approach to mitigating DDoS attacks is the method proposed by (Chen et al., 2018), which leverages the hierarchical structure of the Domain Name System (DNS) to filter out malicious traffic before it can overwhelm target servers. This model is implemented on central recursive DNS servers within ISPs, closer to the source of the attack, allowing early interception of the attack traffic. By applying intelligent traffic filters at the child domain level, the attack traffic can be significantly reduced, preventing it from reaching the top-level domain (TLD) servers. The system uses statistical features like Query Rate (QR) and Source IP Space (SIS) to distinguish between normal and abnormal traffic, and the Random Forest Algorithm to accurately classify and filter out malicious queries. This approach not only enhances the detection and mitigation of DDoS attacks but also maintains service availability by reducing the impact of such attacks on the servers.

Other threats

In addition to the well-known threats of malware, phishing, and DDoS attacks, hosting providers also face other emerging and significant threats that require attention, such as include SQL injections, insider threats, and the abuse of new protocols like DNS over HTTPS (DoH). Each of these threats presents unique challenges and can have serious consequences if not properly addressed.

SQL Injections: As indicated in (Lu et al., 2023), SQL injections remain a critical threat to hosting providers, particularly those managing large-scale web applications and databases. SQL injections involve attackers inserting malicious SQL code into input fields, allowing them to gain unauthorized access to or manipulate the database. Traditional detection methods, which often rely on rule-based systems, have proven inadequate in the face of evolving and sophisticated SQL injection techniques. According to (Lu et al., 2023), a novel approach using a deep learning model named synBERT has shown promising results in detecting SQL injection attacks. By embedding semantic information from SQL statements into a deep learning model, synBERT significantly improves the accuracy and generalization of detection, achieving accuracy rates exceeding 90%. This advancement highlights the need for hosting providers to adopt more sophisticated detection methods to safeguard their databases against SQL injection attacks.

Insider Threats: Insider threats represent a unique challenge in cybersecurity, as they involve individuals within an organization who misuse their legitimate access to cause harm. (Greitzer & Hohimer, 2011) emphasize that insider threats are particularly difficult to detect because they often involve behaviors that do not immediately appear suspicious. The complexity of insider threats lies in the fact that the individuals involved are trusted members of the organization, making it challenging to distinguish between normal and malicious activities. Greitzer and colleagues propose a behavioral modeling approach that integrates various indicators, such as psychological and organizational factors, to predict and mitigate insider threats. This approach is crucial for hosting providers, as they manage sensitive infrastructure that could be compromised by insider attacks. By incorporating behavioral indicators into their security frameworks, hosting providers can proactively address insider threats before they manifest into significant security breaches(Greitzer & Hohimer, 2011).

DNS Over HTTPS (DoH) Abuse: The adoption of DNS over HTTPS (DoH) is intended to enhance privacy by encrypting DNS queries, thus preventing eavesdropping and manipulation. However, this protocol also introduces new challenges for hosting providers, as it can be exploited by malicious actors to bypass traditional DNS filtering mechanisms. The report on (Hynek et al., 2022) outlines how

attackers use DoH to mask their activities, making it difficult for traditional security systems to detect command-and-control communications, phishing, and data exfiltration. This abuse of DoH highlights the double-edged nature of emerging technologies—while they offer significant privacy benefits, they also create new avenues for cyber threats. Hosting providers must adapt to these changes by implementing enhanced monitoring and threat intelligence capabilities to detect and mitigate the misuse of DoH.

2.2.2. Malware as a focus

While every kind of threats presents unique challenges, malware is regarded as one of the most significant and complex threats to hosting environments due to its widespread impact and diverse methods of exploitation.

Malware poses a significant threat to hosting environments due to its prevalence, severity, and regulatory implications. It often uses legitimate websites to spread. (Chang et al., 2013) explains that attackers target trusted websites by exploiting their weaknesses, turning them into platforms for spreading harmful content. This not only damages user trust but also harms the reputation of hosting providers, as even secure websites can become conduits for malware. Malware exploits server resources, causing long-term performance degradation and increasing maintenance costs. Furthermore, as shown in (W. Niu et al., 2019) , malware compromises data, enabling activities such as identity theft and financial fraud, which can be harmful for individuals and organizations.

Moreover, malware significantly impacts hosting environments by exploiting vulnerabilities in shared hosting setups. As illustrated in (Mirheidari et al., 2012), multiple websites shared the same server infrastructure with insufficient isolation between accounts allows malware to spread from one compromised site to another. Attackers often use such weaknesses to manipulate server resources and gain unauthorized access, creating opportunities to distribute the malicious software further(Mirheidari et al., 2012).

The cascading effects of malware also extend beyong the initial infection of the hosting servers. For instance, (Zhou et al., 2008) indicates that botnets constructed from compromised servers are frequently employed in DDoS attacks, which overwhelm targeted servers with malicious traffic, causing widespread outages and significant service disruptions. In addition to enabling DDoS attacks, malware attacks also play a key role in phishing campaigns by hosting fraudulent websites that trick users into sharing sensitive information like passwords or financial details (Zhou et al., 2008).

2.3. Evolution of cyber threats

As the internet environment has evolved, the threats hosting providers are facing also became more complex, driven by advancements in technology. In this section, how cyber threats became more sophisticated and how the advanced technology has been leveraged in cyber threats will be explored.

2.3.1. Trends in attack methods

According to the study by (Akella et al., 2023), the frequency and complexity of cyber-attacks have increased dramatically. Cyber threats has became more targeted and precise. For example, as reported in (Ventures, 2021), there were 800,000 cyber attacks in a single year, which can be averaged in to an attack per 39 seconds. This amount of attacks can lead to large scale of data loss, which can lead to financial losses, violation of privacy and identity theft, etc. The research emphasizes that

bot activity, a critical aspect of contemporary cyber threats, has seen a marked increase, with cybercriminals increasingly leveraging automated systems to execute large-scale, targeted attacks. In 2022 alone, ”bad web bots” were responsible for 17% of all API attacks, often exploiting API business logic to compromise accounts or access sensitive data. Notably, these automated bots contributed to 35% of account takeovers, with attackers using sophisticated methods to avoid detection. This surge in bot-driven cyberattacks is not confined to a single industry; the travel (24.7%), retail (21%), and finance (12.7%) sectors have been particularly impacted. Additionally, sectors such as gaming (58.7%) and telecommunications (47.7%) have experienced overwhelming levels of detrimental bot traffic. The increase in bot attacks is further evidenced by geographical hotspots, with countries like Germany, Ireland, and Singapore showing significantly higher than average bot activity. (Akella et al., 2023).

(Rajasekharaiah et al., 2020) also discussed how the rise of new technologies has introduced vulnerabilities. For instance, the proliferation of Internet of Things (IoT) devices has significantly expanded the attack surface. These devices can be easily targeted by ransomware and other malware due to the lack of robust security measures. Similarly, the study highlights the advancement of social engineering attacks, such as phishing, which now account for 32% of confirmed data breaches. These attacks have become more challenging to detect, especially with advancements in machine learning and AI. Furthermore, the large scale of mobile device usage has introduced new risks as well; for example, (Rajasekharaiah et al., 2020) mentioned that RSA reported an 80% increase in fraudulent mobile transactions in 2018, indicating how mobile platforms are becoming major targets. This growing complexity in attack methods necessitates a corresponding evolution in defense strategies to protect digital assets effectively.

2.3.2. The growing complexity of cyber crimes

The complexity of cybercrimines has grown due to the advancement of technology. As discussed by (Akella et al., 2023), modern cyber threats are characterized by their precision and adaptability. Cybercriminals nowadays employ more advanced techniques such as artificial intelligence and machine learning to enhance their attacks. These technologies allow attackers to automate the process of finding vulnerabilities, make more legit-looking phishing emails, and evade detection by traditional security systems.

(Rajasekharaiah et al., 2020) further elaborates on the role of emerging technologies in the evolution of cyber threats. The study shows how cybercriminals are using AI more to develop new attack methods that are more difficult to detect and defend against. For instance, AI-driven attacks can improve tactics based on the defenses they have encountered, making the countermeasures less effective. The use of AI also enables cybercriminals to conduct large-scale attacks with greater efficiency, targeting multiple organizations simultaneously and increasing the overall impact of their activities(Rajasekharaiah et al., 2020).

The article (Akinsanya et al., 2024) discusses how the growing complexity of cyber crimes has made improving in cybersecurity strategies neccessary. Traditional defense mechanisms which rely on static security measures, are no longer sufficient to protect against these advanced threats. Instead, there is a need for dynamic, adaptive approaches that can respond to the rapidly changing cyber threats. This includes the integration of resilience into cybersecurity strategies, focusing on not only preventing attacks but also detecting, responding to, and recovering from them (Akinsanya et al., 2024).

The evolution of cyber threats shows that it is important for organizations, particularly hosting providers,

to stay ahead of the curve by adopting advanced security measures and continuously improving their cybersecurity frameworks.

2.3.3. Adapting to the evolution of cyber threats

The increasing consolidation of DNS and web hosting providers has been a key driver in the significant evolution of cyber threats, which have become more sophisticated and widespread as internet technologies continue to grow. As internet traffic becomes increasingly centralized among a few dominant providers, the associated cybersecurity risks are amplified, making these providers prime targets for cyberattacks (Geer et al., 2020). This consolidation creates both challenges and opportunities for hosting providers, as they must adapt to an environment where the stakes are higher, and the potential for widespread disruption is greater.

The nature of cyber threats has also changed in response to advancements in defensive technologies. As security measures have become more robust, threat actors have developed new methods to bypass them. For instance, (Muir & Oorschot, 2009)explain how attackers use techniques like geolocation evasion and rely on decentralized infrastructures such as VPNs and TOR networks to hide their activities. These strategies make it increasingly challenging for hosting providers to track attackers and respond effectively to cyber threats.

To adapt to these evolving threats, hosting providers have had to innovate continuously. (Tasnim et al., 2022) discussed how centralized security measures, such as global threat intelligence sharing and automated incident response systems, have been crucial in managing the heightened risks associated with greater centralization. Furthermore, (Apruzzese et al., 2023) note that hosting providers are increasingly utilizing real-time data analysis and machine learning to detect and respond to threats more quickly and accurately. This shift towards more proactive and adaptive security strategies represents a significant evolution in how hosting providers protect their infrastructure and clients.

Despite these advancements, the consolidation of DNS and web hosting services also presents new risks. The potential for large-scale outages or targeted attacks on key infrastructure components means that hosting providers must remain vigilant and continuously update their security protocols to address emerging threats. The ongoing evolution of cyber threats requires a dynamic and flexible approach to security, one that can keep pace with the ever-changing landscape of cybercrime.

2.4. The role of hosting providers in preventing abuse on their networks

Hosting providers are a key component in maintaining the internet as a safe and reliable space, but this requires them to actively monitor and manage their networks to prevent abuse. Early detection systems play a vital role in this effort by identifying threats like compromised websites, which can be used for malicious purposes if not addressed promptly (Canali et al., 2013). Collaborative efforts are equally important, as providers that share information about abuse with others tend to see significant improvements in reducing malicious content, such as harmful URLs, across their networks (Vasek et al., 2016).

The challenges do not stop there. Poorly monitored hosting environments can become safe havens for harmful activities, including financial malware that relies on command-and-control infrastructures. When hosting providers maintain a strong oversight of their networks, they are able to disrupt these

infrastructures and minimize their impact on users and businesses (Tajalizadehkhoob et al., 2017). At the same time, networks that neglect monitoring often end up facilitating ”bulletproof hosting,” where illegal activities can thrive undetected. (Alrwais et al., 2017) stress the importance of close monitoring, especially of traffic patterns, to address this growing issue. Furthermore,(Fryer et al., 2015) suggest that many providers are not fully utilizing their potential to prevent abuse, as they often overlook opportunities to actively manage and oversee the activities happening within their networks.

When hosting providers prioritize proactive measures and network oversight, they help create a more secure and trustworthy digital ecosystem. Without this effort, networks can become vulnerable to exploitation, which not only undermines the integrity of their services but also endangers the broader online community.

2.5. Geographical compliance and the importance of adhering to the Digital Services Act

For companies based outside EU, adhering to local regulations is crucial if they wish to conduct business in these regions. This ensures that their operations are legally compliant and fosters trust within the digital market. At the same time, Dutch companies must also align with national and EU standards. (Loos, 2021) highlights how the Netherlands has incorporated the Digital Content Directive into its national compliance framework, demonstrating the importance of aligning business practices with evolving EU regulations.

For hosting providers in particular, geographical compliance is essential, as it ensures their services adhere to local laws, enabling them to operate legally while meeting the expectations of regional authorities and users. Such alignment helps hosting providers build trust and maintain their reputation while avoiding potential regulatory conflicts (Alkemade & Toet, 2021).

(Wilman et al., 2024) explains that the DSA’s primary aim is to create uniform regulations across Europe, while still allowing member states to adopt and enforce these rules within their specific legal contexts. (Kamara et al., 2020) further emphasize that Dutch cybersecurity certification practices align closely with EU guidelines, making it easier for companies operating in the Netherlands to meet compliance requirements. Establishing services in regions like the Netherlands is, therefore, not just a legal obligation but also a strategic advantage, offering a clearer pathway to navigate Europe’s complex regulatory landscape.

2.6. The Digital Services Act(DSA) and it provisions

2.6.1. Overview of the Digital Services Act

The Digital Services Act is one of the EU’s digital regulatory framework, with the target of establishing a safer online environment while prioritizing user protection, transparency, and accountability. It was introduced by the European Commission in December 2020 as a part of a broader effort to modernize regulations for digital services across Member States. This initiative emerged from the recognition that the E-Commerce Directive (2000/31/EC), which governed digital services for over two decades, was no longer sufficient to address the complexities of the current digital landscape (Pereira, 2021) (Husovec & Roche Laguna, 2022). (Turillazzi et al., 2023) highlighted its potential to influence global digital policies, particularly in setting standards for transparency and accountability.

2.6.2. Key requirements of the DSA for hosting providers

An important aspect of the DSA is that it sets new and strict obligations on hosting providers. As mentioned in (Quintais & Schwemer, 2022), these providers must meet detailed requirements for transparency in content moderation, systematic reporting on content takedown procedures, and the handling of illegal content. Platforms are required to disclose data regarding the algorithms used in recommendation systems and provide detailed explanations of their content removal processes to enhance user trust and accountability(Quintais & Schwemer, 2022).

The regulation also introduces a system of due diligence obligations based on the size and societal impact of the services as below:

Universal obligations

These apply to all intermediary services, regardless of size. These include providing a point of contact or legal representative, outlining terms and conditions, and ensuring transparency through annual reporting for medium-sized or larger firms (Husovec & Roche Laguna, 2022).

Basic obligations

These apply specifically to hosting providers of all sizes. These obligations include handling notices of illegal content and notifying authorities of serious crimes (Husovec & Roche Laguna, 2022).

Advanced obligations

These are tailored to online platforms that are medium-sized or larger (defined as having more than 50 employees or €10 million in turnover or assets). These platforms must establish trusted flagger systems, manage complaints through internal systems, offer out-of-court dispute resolution, implement repeat infringer policies, ensure fair design and transparency, protect minors, and provide consumer notifications and marketplace compliance mechanisms (Husovec & Roche Laguna, 2022).

Special obligations

These are imposed on Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), defined as platforms with an average of 45 million active monthly users in the EU. These obligations include conducting systemic risk assessments, implementing risk mitigation and crisis response protocols, conducting independent audits, and meeting additional requirements related to advertising transparency, recommender systems, data sharing, and compliance functions (Husovec & Roche Laguna, 2022).

2.6.3. Specific requirements for hosting providers

Hosting providers are subjected to the requirements outlined in the DSA asided from the tiered obligations.

The DSA classifies providers into distinct categories, each subject to specific obligations based on their size, societal impact and type of service they provide. Intermediary services facilitate network access or data transmission, like ISPs and cloud infrastructure. Hosting services store and manage user content, such as web hosting providers. Online platforms actively distribute user content, including social media platforms like Facebook. Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) are platforms or search engines with over 45 million monthly active users, such as Facebook, TikTok, Google, and Bing, which face stricter compliance requirements. The type of obligations the providers need to meet are summarized in Table 2.1,Table 2.2 and Table 2.3, and the different type of providers are subjected to different specific requirements, this is presented in Table 2.4 from (European Parliament and Council of the European Union, 2022).

2.6.4. Penalities for non-compliance

When not complying to the regulation in DSA, companies may face some panelities according to (European Parliament and Council of the European Union, 2022). they can receive a fine up to 6 In the case that users or other parties affected experience damages due to a provider's non -compliance, they have the right to seek for compensation under the DSA as stated in Article 54. For serious breaches, particularly involving VLOPs and VLOSEs, the providers are required to submit action plans detailing the steps they will have to take to correct the breach. This plan will be reviewed by European Commission, which monitors the implementation to ensure compliance(European Parliament and Council of the European Union, 2022). The European Commission has the power to perform on-site audits if the providers fail to cooperate, as stated in Article 54. DSA introduces a limitation period of five years for imposing penalties, starting from the date of the infringement (Article 56(1)). If the infringement is ongoing, the limitation period starts from the date the infringement ends. For enforcement of penalties (such as payment of fines), a separate five-year limitation period applies (Article 56(2))(European Parliament and Council of the European Union, 2022). The limitation period can be interrupted or suspended if the Commission takes action to enforce payment or requests judicial intervention (Article 56(3))(European Parliament and Council of the European Union, 2022).

2.7. Timeline for Digital Services Act

In (European Commission, 2022), the timeline of the DSA is summarized Figure 2.1, this timeline serves as a critical reference for identifying the date of implementation of the DSA, which is essential for testing the differences in outcomes before and after its enforcement.

2.8. Key takeaways of the literature review

This chapter reviewed existing research on abuse mitigation, the role of the Digital Services Act (DSA), and the cybersecurity challenges faced by Dutch hosting providers. The literature shows that cyber threats like malware and phishing remain persistent problems, and while hosting providers play a key role in fighting abuse, regulations alone may not be enough to reduce malicious activity. Several studies highlight that compliance frameworks like the DSA help improve transparency and accountability, but they do not always lead to better security outcomes. Factors such as the resources available to hosting providers, enforcement consistency, and the ability of cybercriminals to adapt all influence how effective these regulations are in practice.

The literature also emphasizes that hosting providers do not work in isolation—law enforcement, regu-

Figure 2.1: DSA compliance timeline

lators, security professionals, and end users all contribute to abuse mitigation. However, the extent of their cooperation varies, which can create gaps in enforcement. The research reviewed in this chapter points to a need for more studies that examine whether compliance with the DSA actually improves cybersecurity in measurable ways. There is limited research on how hosting provider size, business focus, and compliance efforts affect their ability to reduce malicious activity.

Article	Title	Compliance Obligation	Practical Checkpoints	Data Source / Evidence
Article 10	Point of Contact	Hosting providers must designate a single point of contact for users, authorities, and regulators.	1. Point of Contact listed on website. 2. Email or phone number for direct communication.	Website (Contact Us / Legal Notice)
Article 11	Legal Representative	Providers without EU establishments must designate an EU legal representative.	1. Is a legal representative named and accessible?	Legal Documents (Privacy Policy, T&Cs)
Article 12	Transparency of T&Cs	T&Cs must be clear, explain rules on illegal content, moderation, and recommender systems.	1. Clarity of T&Cs on removal of illegal content. 2. Do the T&Cs explain moderation and recommender system logic?	Terms & Conditions (T&Cs)
Article 13	Notification of Changes	Users must be informed of major changes in T&Cs that affect their usage rights.	1. Do users receive notifications of T&C changes?	Email Alerts / User Notifications/Check what is in the Service Level Agreement
Article 16	Notice & Action	Hosting providers must have an accessible system to report illegal content.	1. Is there a Report button? 2. User submission form with clear instructions.	Report Forms on the website / User FAQ
Article 17	Statement of Reasons	Hosting providers must notify users when removing or restricting access to content.	1. Are users informed about takedown reasons? 2. Is there a system to receive and view takedown notifications?	Email Notifications / Alerts in User Account/Service Level Agreement
Article 18	Criminal Offense Notification	Providers must report suspected criminal offenses that threaten life/safety to authorities.	1. Does the provider have a policy for notifying law enforcement?	Compliance Policy / Transparency Report
Article 20	Complaint Handling	Providers must provide complaint-handling mechanisms for users.	1. Is there a complaint submission system? 2. Are appeals possible?	Appeals Forms / User Complaint Submission
Article 21	Dispute Resolution	Hosting providers must participate in out-of-court dispute resolution.	1. Are there guidelines for dispute settlement? 2. Are bodies for out-of-court settlement listed?	Terms & Conditions (T&Cs) / Legal Policy

Table 2.1: Compliance Obligations and Practical Checkpoints for DSA Articles (Part 1)

Article	Title	Compliance Obligation	Practical Checkpoints	Data Source / Evidence
Article 24	Transparency Reporting	Providers must publish annual transparency reports on moderation activity.	1. Does the provider publish a transparency report? 2. Is the report downloadable?	Transparency Reports section on website
Article 20	Anti-Abuse Systems	Providers must implement measures to prevent misuse (e.g., spam, abuse).	1. Does the provider have IP blacklists or account lockout systems?	Abuse Policy / Security Policy
Article 22	Trusted Flaggers	Providers must recognize and give priority to trusted flaggers for illegal content.	1. Does the provider prioritize reports from trusted flaggers?	Transparency Report / User Guides
Article 23	Notice Transparency	Providers must inform users of the status of illegal content reports.	1. Can users track the status of their content reports?	User Dashboards / Email Notifications
Article 26	Ad Transparency	Ads must be labeled clearly, and info on sponsors must be disclosed.	1. Are ads labeled as Sponsored or Ad ? 2. Are advertisers listed?	Advertising Policy / Ad Labels on Platform
Article 27	Recommender Transparency	Providers must offer control over how recommendations are personalized.	1. Are there user controls for recommendation preferences?	User Profile Settings / Account Preferences
Article 34	Risk Assessments (VLOPs)	VLOPs must conduct risk assessments for systemic risks (disinformation, minors' safety, etc.).	1. Are risk assessments published? 2. Is there evidence of risk mitigation?	Risk Mitigation Reports / Compliance Policy
Article 37	External Audits (VLOPs)	VLOPs must undergo independent audits annually.	1. Does the provider have an external audit report?	Audit Reports External Audit Summary

Table 2.2: Compliance Obligations and Practical Checkpoints for DSA Articles (Part 2)

Article	Title	Compliance Obligation	Practical Checkpoints	Data Source Evidence
Article 40/41	Data Sharing	Providers must share data with authorities and researchers as required.	1. Is there a clear data-sharing policy? 2. Does the provider comply with national orders for data?	Data Sharing Policy Privacy Policy
Article 45	Code of Conduct	Providers may voluntarily join EU Codes of Conduct (e.g., Disinformation Code).	1. Is the provider a signatory of any DSA-related Code of Conduct?	News Announcements Provider Statements
Article 48	Crisis Cooperation	Providers must cooperate with authorities in times of crisis.	1. Is there a crisis response plan or emergency contact point?	Compliance Reports Transparency Reports
Article 52	Sanctions for Non-Compliance	Providers face fines and penalties for failing to meet obligations.	1. Has the provider faced any sanctions or fines under the DSA?	Regulatory Fines Compliance Reports

Table 2.3: Compliance Obligations and Practical Checkpoints for DSA Articles (Part 3)

Table 2.4: Provider Types and Key Obligations under the DSA

Provider Type	Definition	Key Obligations	Relevant Articles
Mere Conduits	Transmit data without storing or altering it (e.g., ISPs).	- Liability exemption if passive. - Designate a point of contact. - Appoint a legal representative (if outside EU).	4, 8, 10, 11
Caching Services	Temporarily store data to optimize delivery (e.g., CDNs).	- Liability exemption if unaltered. - Remove illegal content upon notice. - Designate a point of contact. - Appoint a legal representative.	5, 8, 10, 11
Hosting Services	Store user-provided content (e.g., web hosting, cloud hosting, VPS).	- Liability exemption for illegal content if removed upon notice. - Notice-and-action mechanisms. - Transparency reporting. - Statement of reasons for removals. - Point of contact - Transparenct of Terms & Conditions - legal representative.	6, 8, 10, 11, 14, 15, 24
Online Platforms	Host and disseminate public content (e.g., social media platforms, marketplaces).	- Same as hosting services, plus: - Trusted flagger systems. - Internal complaint handling. - Recommender system transparency. - Protection of minors.	6, 8, 10, 11, 14, 15, 17, 22, 27, 28
VLOPs and VLOSEs	Platforms or search engines with over 45 million monthly active EU users (e.g., Facebook, TikTok, Google, Bing).	- Same as online platforms, plus: - Systemic risk assessments. - Risk mitigation measures. - Annual independent audits. - Data sharing with regulators. - Transparency in advertising systems.	6, 8, 10, 11, 14, 15, 17, 22, 24, 27, 34, 37, 40

3

Methodology

3.1. Research design and approach

This study adopts a quantitative analysis method to evaluate the impact of the Digital Services Act (DSA) on Dutch hosting providers' anti-abuse practices. The overall research design follows a structured, multi-phase framework to ensure a systematic and comprehensive evaluation. As illustrated in Figure 3.1, Figure 3.2 and Figure 3.3, the study progresses through six distinct phases: problem definition, objective setting and methodology development, data collection and preprocessing, data analysis and hypothesis testing, and interpretation and reporting of results.The analysis begins with large-scale passive DNS data, which is used to map domain names to IP addresses, specifically Fully Qualified Domain Names (FQDNs). Hosting providers are classified based on their IP address distribution, size of infrastructure, and their association with malicious behavior. This classification is critical for identifying patterns and trends in abuse levels across the selected providers.

The first step is defining Dutch hosting providers using the datasets, which include detailed attributes such as total IP addresses, Netherlands-specific IPs (NL IPs), Fully Qualified Domain Names (FQDNs), Second-Level Domains (SLDs), and organization names. These attributes allow for the classification of providers based on size, scope, and operational presence in the Netherlands. By narrowing the focus to providers with substantial infrastructure in the Dutch market, the analysis ensures that the study remains relevant to the regulatory context of the DSA.

To evaluate changes in malicious IP activity, data from January 2023 to April 2024 is analyzed using Interrupted Time Series (ITS) analysis, which assesses both immediate and gradual changes in malicious IP percentages following the DSA's enforcement in February 2024. This method accounts for pre-existing trends and isolates the effects of the regulation.

To measure compliance with the DSA, a compliance scoring framework is applied. The obligations outlined in the DSA, such as notice-and-action mechanisms, transparency reporting, and points of contact, are operationalized into measurable criteria. For each hosting provider, compliance is assessed by examining publicly available information, such as transparency reports and policies, to determine whether they meet these requirements. Each requirement is scored as either met (1) or unmet (0),

and a compliance score is calculated as the proportion of requirements fulfilled relative to the total applicable to the provider.

Multivariate regression models explore the relationships between compliance scores, hosting provider characteristics (e.g., size and client focus), and malicious IP percentages. This approach examines whether compliance with the DSA and provider-specific traits influence the level of malicious activity, offering valuable insights into the regulatory framework's effectiveness.

This study validates the results through comparisons with existing research, ensuring that the findings are consistent with broader trends and challenges in cybersecurity regulation. Aligning the outcomes with existing studies helps the research demonstrate its relevance to ongoing discussions about regulatory effectiveness. This approach strengthens the study's validity by placing its findings within the wider context of existing knowledge while emphasizing its unique contributions to understanding the impact of the DSA

3.2. Data sources and collection

To analyze the impact of the Digital Services Act (DSA) on hosting providers, data was collected from multiple authoritative sources. The passive DNS dataset was provided by TU Delft as part of an academic collaboration. This dataset was chosen due to its extensive coverage of domain resolution history, allowing for the identification of trends in domain-to-IP mappings, which is crucial for assessing changes in malicious activity pre- and post-DSA implementation (January 2023 – April 2024). The use of passive DNS was agreed upon due to its reliability in tracking historical domain resolutions and its non-intrusive nature, making it an ethical and scalable method for studying malicious infrastructure.

The dataset includes several key attributes for each hosting provider, allowing for a detailed evaluation of its infrastructure and activity. These attributes include the total number of IP addresses controlled by each organization, as well as the number of IP addresses specifically associated with the Netherlands. To assess the extent of each provider's presence in the Dutch hosting market, the percentage of its total IPs located in the Netherlands was calculated. Additionally, the dataset captures domain-level data, including the total number of Fully Qualified Domain Names (FQDNs), which represent individual subdomains linked to a provider, and the total number of Second-Level Domains (SLDs), which indicate root domains controlled by the organization.

To identify malicious IP addresses, data was retrieved from well-established threat intelligence feeds, including Spamhaus, AbuseIPDB, and Shodan. These sources maintain up-to-date blacklists of IP addresses linked to spam, phishing, malware distribution, and other abusive activities. IP addresses flagged as malicious in these databases were cross-referenced with the passive DNS dataset to determine their association with Dutch hosting providers.

To develop the compliance matrix and assess compliance levels, publicly available sources such as terms of service, abuse policies, and transparency reports published by hosting providers were examined.

3.3. Defining dutch hosting providers

This step will give the definition of what is a dutch hosting provider. First the organization needs to have a significant proportion of IPs located in the Netherlands. Organisations are non-hosting companies will be excluded in the research, such as companies hosting for their own use.

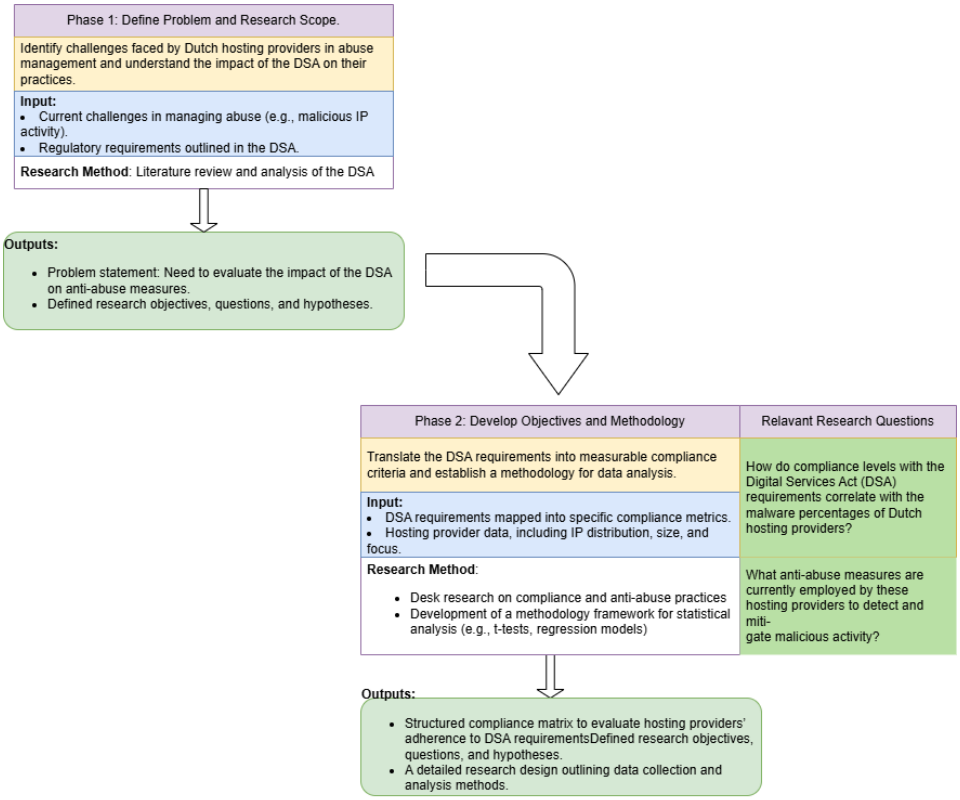

Figure 3.1: Flowchart-1

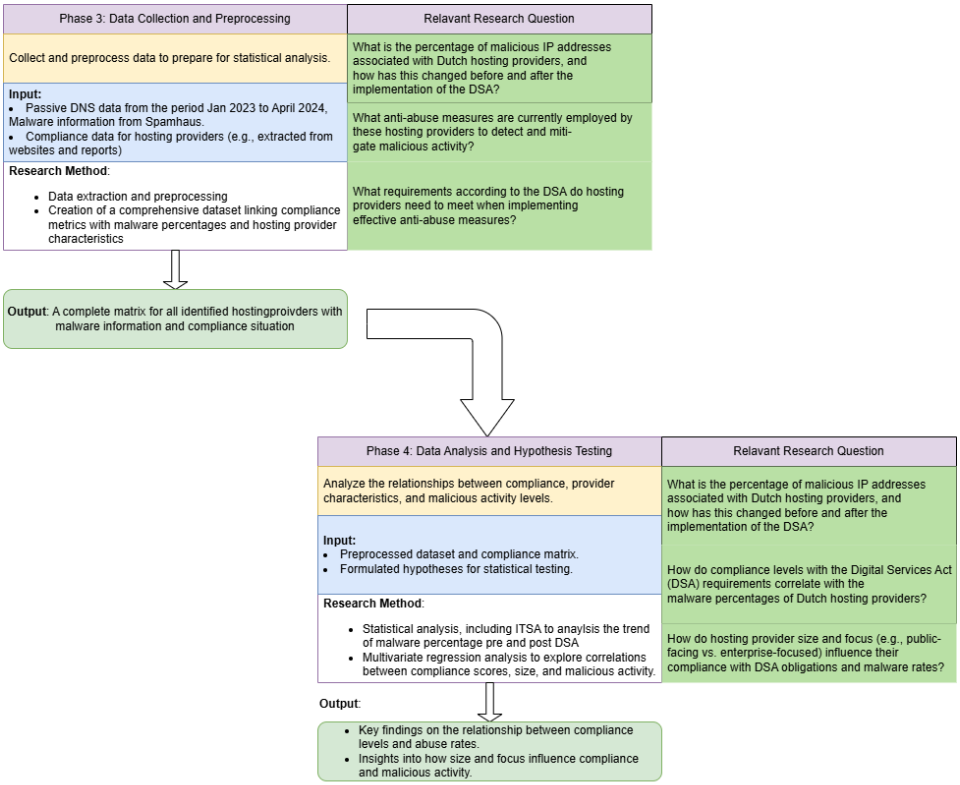

Figure 3.2: Flowchart-2

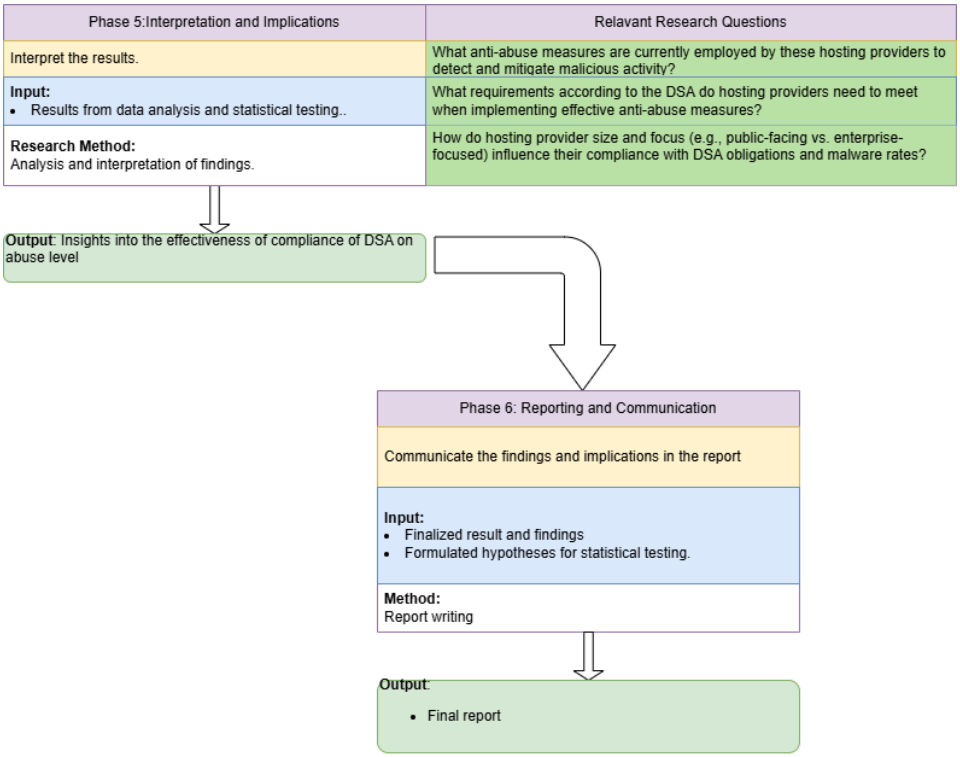

Figure 3.3: Flowchart-3

3.3.1. Hosting vs. Non-Hosting Entities

This step will select the hosting entities that are relevant for this research. Organizations such as Vodafone and Airtel Broadband, which primarily operate as ISPs (Internet service providers) or CDNs (Content delivery networks), will be excluded from the definition of hosting providers. Although these entities control large blocks of IPs, they do not provide traditional hosting services. As outlined in the research (Tajalizadehkhoob et al., 2016), abuse-handling practices and infrastructure responsibilities differ significantly between hosting providers and other network service entities.

Defining hosting providers

In this research, hosting providers are defined as entities primarily offer services that allow individuals or businesses to host websites, applications, and content online on infrastructure that they do not own. According to Tajalizadehkhoob et al., 2016, hosting providers play a role in renting out hardware and network access to end users who need a platform to create an online presence. This definition provides a focus on providers who are responsible for monitoring and controlling the content hosted on their infrastructure; they are more directly involved in mitigating abuse.

Excluding non-hosting entities

Non-hosting entities such as ISPs and CDNs are excluded from this research.

Internet Service Providers(ISPs) primarily provide connectivity services to end-users rather than web hosting. Their focus is on transmitting data across networks rather than hosting content. While ISPs do manage IP address allocations, they typically do not control or monitor the content hosted by their customers. Therefore, including ISPs would misalign the research scope, as ISPs' responsibilities and actions concerning abuse handling differ from those of dedicated hosting providers.

CDNs are designed to optimize the delivery of web content by caching it closer to end-users. While they do host content temporarily for performance optimization, their primary role is not to provide a permanent hosting solution. CDNs like Cloudflare and Amazon CloudFront generally do not have the same level of control over the content origin as traditional web hosting providers, as their role is to facilitate fast and efficient content delivery rather than to serve as the main host. Including CDNs would introduce entities whose abuse control practices are generally focused on performance and security at the network edge, rather than on direct content hosting responsibilities.

Some organizations may have a significant online presence but are not service providers for others. These companies may appear in the dataset with large numbers of IPs or domains; however, they use their infrastructure solely for their own operations, not to host third-party content. Including such organizations would be irrelevant for a study focused on hosting providers who manage abuse from external clients. Therefore, companies that manage their own content without offering hosting services to others will also be excluded.

The following manual selection method is developed based on the information above in order to select the relevant hosting providers for this research:

- The primary hosting services will be checked, check if the website mentions clearly about web hosting, cloud hosting, VPS, or dedicated hosting.
- Make sure the provider provides service to third-parties instead of only for internal use.
- Ensure they offer a range of hosting solutions, not just auxiliary or consulting services.

3.3.2. Measuring Abuse Through Malware and IP Tracking

Hosting providers face the challenge of balancing client privacy with their responsibility to secure the infrastructure they manage. While clients have the right to confidentiality, hosting providers remain accountable for any malicious activity occurring on their network—whether initiated by a client through negligence or via exploitation by hackers. This creates a delicate situation where providers cannot directly inspect or eavesdrop on client data but must still maintain robust controls to detect and mitigate abuse.

Malware serves as a critical predictor in this context because it provides observable technical traces, such as unusual traffic patterns, resource spikes, or connections to malicious domains. These indicators can be monitored without compromising client privacy, making malware detection a widely accepted method for identifying abuse. Given that malware dissemination and command-and-control infrastructure are primarily tracked through IP addresses, the percentage of malicious IPs associated with a hosting provider becomes a natural and effective metric for evaluating abuse levels.

Unlike domains, which can be rapidly created and discarded using Domain Generation Algorithms (DGAs), IP addresses provide a more stable and consistent identifier in abuse monitoring. While domains change frequently to evade detection, IPs tend to remain assigned to specific hosting providers for longer periods, making them more suitable for longitudinal analysis. Additionally, malware threat intelligence feeds, such as Spamhaus and AbuseIPDB, primarily report abuse at the IP level, reinforcing its role as a standard metric in cybersecurity research.

Although tracking malicious domains could offer complementary insights, the large volume and dynamic nature of domain abuse exceed the computational and analytical capacity of this study. Incorporating domain-based analysis would require larger datasets, advanced clustering techniques, and more ex-

tensive filtering mechanisms to distinguish legitimate from malicious use. Given these constraints, this research focuses on IP-based abuse detection as a scalable, reliable, and widely accepted approach to evaluating hosting provider security practices. Future research could extend this work by incorporating domain-level abuse metrics to provide a more granular view of infrastructure exploitation.

3.4. Compliance matrix

The evaluation of compliance with the Digital Services Act (DSA) was carried out by translating its requirements into measurable criteria. Hosting providers, defined in Section 3.3.1, were assessed for adherence to core obligations such as notice-and-action mechanisms, transparency reporting, statements of reasons for removals, points of contact, and legal representatives. This process relied on identifying the specific requirements applicable to each provider type, operationalizing those requirements into measurable indicators, and using a compliance matrix to analyze results.

The first step in the process was to analyze the text of the DSA itself to determine what obligations applied to hosting providers. From this analysis, key questions emerged to guide the compliance evaluation. For instance, determining whether a provider had a published notice-and-action mechanism for illegal content or whether it offered a clear statement of reasons for content removal were essential points of inquiry. The identification of observable evidence, such as website content, published reports, or stated policies, provided a practical basis for assessing compliance. By focusing on these indicators, it was possible to systematically evaluate how well providers adhered to the requirements.

To organize this information, a compliance matrix was developed. This matrix quantified compliance by scoring providers with a ”1” for meeting a requirement and a ”0” for failing to do so. The overall compliance score for each provider was calculated as the ratio of requirements met to the total number of requirements applicable to them. In addition to compliance scoring, the matrix included details about each provider’s focus, such as whether their services were public-facing or enterprise-focused, and information on malware percentages associated with the provider. This structure allowed for the integration of compliance data with performance metrics for further statistical testing.

The DSA’s varying obligations for different types of hosting providers required a mapping process to match requirements with provider categories. Table 2.4 was created to classify providers based on the DSA’s definitions, such as hosting services, online platforms, or very large online platforms, and their corresponding requirements. These classifications were then aligned with the specific definition of hosting providers used in this research, allowing for the identification of relevant obligations for each type of provider and ensuring the requirements were accurately incorporated into the compliance matrix.

Compliance assessment was conducted through desk research, where publicly available information was systematically reviewed. This included providers’ websites, published reports, terms of service, and policies related to notice-and-action procedures. A provider, for example, was considered compliant with the notice-and-action requirement if a clear and operational mechanism was accessible on their platform. This method ensured that the assessment was grounded in observable, verifiable evidence.

The compliance matrix plays an important role in the statistical analysis by linking compliance scores to malware data. Establishing the DSA’s implementation timeline provided a critical reference point for distinguishing pre- and post-enforcement conditions. This approach allows for the evaluation of how compliance with the DSA has impacted hosting providers and enables comparisons of key metrics to analyze its overall effect.

3.5. Hypotheses

Sub-question 1: What is the percentage of malicious IP addresses associated with Dutch hosting providers, and how has this changed before and after the implementation of the DSA?

- H0: There is no significant difference in malware percentages before and after the implementation date of the DSA.

- H1: Malware percentages decreases after the DSA.

Sub-question 2: How do compliance levels with the Digital Services Act (DSA) requirements correlate with the malware percentages of Dutch hosting providers?

- H0: There is no relationship between compliance scores and malware percentages.

- H1: Higher compliance scores correlate with lower malware percentages.

Sub-question 5: How do hosting provider size and focus (e.g., public-facing vs. enterprise-focused) influence their compliance with DSA obligations and malware rates?

- H0: Hosting provider size and focus have no significant influence on their compliance with DSA obligations or malware rates.

- H1: Hosting provider size and focus significantly influence their compliance with DSA obligations and malware rates.

3.6. Statistical analysis framework

To understand the impact of the Digital Services Act (DSA) on malicious IP percentages and the factors that influence them, this study used a combination of Interrupted Time Series (ITS) analysis and multiple regression models. ITS analysis was chosen to examine how malware percentages changed before and after the DSA was implemented. This method is ideal for analyzing policy changes because it can separate the effects of the intervention from any trends that were already happening. The ITS model included three main elements: a time variable to track changes in malware percentages over the study period, a post-DSA indicator to show whether an observation occurred before or after the DSA, and an interaction between time and the post-DSA period to determine whether the DSA affected the trend over time. This allowed the analysis to assess both immediate changes in malware percentages and any longer-term effects on their trajectory.

In addition to ITS, multiple regression models were used to explore how specific factors, such as compliance scores, provider size, and client focus, influenced malware percentages. Compliance score measured how well hosting providers followed DSA rules. Provider size was calculated based on the average number of IP addresses managed by each provider, while client focus was categorized as either public-facing or enterprise-focused. Seven models were created to analyze these relationships. The first two models looked at compliance score and provider size separately. The third model tested their combined effects, while the fourth model added an interaction term to see if provider size influenced the relationship between compliance score and malware percentage. The last three models included client focus as an additional factor, testing whether it directly impacted malware percentages and how it interacted with the other predictors.

Each model was evaluated using several statistical measures. Regression coefficients were used to understand the direction and size of the relationships, p-values tested whether these relationships

were statistically significant, and R-squared values measured how much of the variation in malware percentages could be explained by the model.

This chapter outlined the methodological approach used to assess the impact of the Digital Services Act (DSA) on abuse mitigation among Dutch hosting providers. The study employs passive DNS data to track changes in malicious IP activity before and after the DSA's implementation, while compliance levels are analyzed to determine their relationship with malware prevalence. To evaluate these trends, the research uses Interrupted Time Series (ITS) analysis and regression models, which help measure whether compliance with the DSA leads to a significant reduction in cyber threats.

The methodology was designed to provide a structured and data-driven approach to answering the research questions. ITS allows for the examination of time-based trends, controlling for existing patterns, while regression analysis helps explore the correlation between compliance and malicious activity.

The methodology provides the basis for the analysis in the next section. The methods chosen allow for a systematic evaluation of the DSA's effectiveness, helping to determine whether compliance translates into better cybersecurity outcomes. The findings in the following chapter will provide key insights into how hosting providers manage abuse and whether regulatory measures like the DSA are making a measurable difference in reducing cyber threats.

4

Analysis and Results

4.1. Filtering strategy

The data generated from the input is presented in CSV format at /home/data/people/meixuan/preselection. In order to select dutch hosting providers based on the strategy mentioned in the methodolgy, a filtering mechanism will be applied. The filtering is conducted in R Studio, with the code available on Zenodo (M. Niu, 2024)

Step 1: Filter by ”Percentage of NL IPs” The Percentage of NL IPs is the most straightforward metric for identifying providers with a significant presence in the Netherlands. To ensure that only providers with a meaningful footprint in the Netherlands are focused on, apply the following filters:

High NL Presence: Set a threshold of 5% or more of NL IPs. This argues a noticeable amount of business/services the hosting providers offer in the Netherlands, making them relevant for this research Examples: SingleHop LLC (12.53%), Digital Ocean (11.57%), xTom (10.32%).

Step 2: Remove Non-Hosting Providers Some organizations might be ISPs, CDNs, or other types of service providers that do not primarily provide hosting services. Since this research focuses on organizations offering hosting solutions, such as virtual private servers (VPS), dedicated hosting, and shared hosting, these non-hosting providers will be excluded.

Providers with high total FQDNs (more than 10,000) and SLDs (more than 1,000) are included in this study because these metrics are robust proxies for significant hosting activity across diverse types of hosting services. While high FQDN and SLD counts are often associated with web hosting, they also reflect broader hosting operations, including VPS and dedicated hosting providers. These counts indicate a provider’s capacity to host a large and active client base, whether through domains for websites or infrastructure for applications and backend systems.

Even in cases where VPS or dedicated hosting providers might host fewer domains compared to traditional web hosting, those meeting these thresholds show an extensive operational scope, which increase their relevance to the study. For instance, a provider with high FQDN and SLD counts is likely to indicate diverse clients, some of whom may utilize the hosting infrastructure for applications or enterprise-level services rather than public-facing websites.

Step 3: After filtering providers by their percentage of NL IPs and excluding non-hosting entities, a manual online search is conducted to verify that the remaining providers are primarily involved in hosting services, including web hosting, VPS, dedicated hosting, and public cloud hosting. This step ensures that only providers relevant to the research are included in the analysis.

Organizations such as Vodafone, Airtel Broadband, Ziggo, KPN, and SURF BV are excluded because they primarily operate as Internet Service Providers (ISPs) or telecommunications companies. These entities focus on delivering internet connectivity, telephony, and network services rather than offering specialized hosting services to clients. While some of these companies may have hosting capabilities, these are often supplementary to their primary operations and do not constitute the primary focus of this research, which examines hosting providers directly responsible for hosting client infrastructure, content, and applications.

Similarly, organizations like Amazon CloudFront and other Content Delivery Networks (CDNs) are excluded because their primary function is to optimize the delivery of web content by caching it closer to end users. CDNs typically act as intermediaries in delivering content hosted elsewhere and do not directly manage or control client infrastructure, making them less relevant to the study's focus on hosting providers and their role in managing potential malicious activity.

Companies such as Accenture B.V. and other organizations that host infrastructure exclusively for their internal operations are excluded. These self-hosting entities do not provide hosting services to external clients, and therefore, they fall outside the scope of this research.

4.2. Data processing and analysis

4.2.1. Preparing the list of dutch hosting providers

The dataset used for this analysis is derived from passive DNS data, which provides a historical and aggregated record of DNS resolutions observed across various networks. Passive DNS is a valuable resource for identifying trends in domain usage, resolving infrastructure associations, and monitoring malicious activity over time. It enables the mapping of Fully Qualified Domain Names (FQDNs) and Second-Level Domains (SLDs) to associated IP addresses, which are critical for analyzing hosting providers' activities.

The raw dataset is processed to generate a monthly list of hosting providers and their corresponding metadata; including total IPs, the number of IPs located in the Netherlands (NL IPs), the percentage of NL IPs, total FQDNs, and total SLDs. Each monthly dataset is filtered using the previously described methodology to ensure consistency and relevance across all data points.

A list of hosting providers is generated for each month from January 2023 to April 2024, based on the filters applied. In the research, the aggregate of these monthly hosting providers is analyzed. The full list can be found in Appendix A.

4.2.2. Mapping of the IPs to hosting providers

A mapping of the IP addresses to and name of the hosting companies is generated for each month and stored in /home/data/people/meixuan/iporg. The code for generating these mappings is available on Zenodo (M. Niu, 2024). A look up is performed for each month for all the hosting providers. Another set of files is created in /home/data/people/meixuan/iprange, containing the final mapping of selected hosting providers and their relevant IPs.

4.3. Analysis of malicious IP percentage

4.3.1. Calculation of the percentage of malicious IPs

The analysis of malicious IP percentages is based on daily IP threat data obtained from Spamhaus, from January 2023 to April 2024. This data, stored in .json.gz format, includes detailed records of malicious IPs, associated threats, and timestamps. The data is processed by matching each IP against a locally stored mapping file that associates IPs with their respective hosting providers and countries. When a match is identified, the script records the company, country, threat type, and detection date, aggregating the results into a structured CSV file. From this aggregated dataset, an additional step was performed to create a refined CSV containing only unique IPs with reported malware and their corresponding company names, these results are stored in /home/data/people/meixuan/uniquemalwareips. The python scripts relate to this step is in Zenodo (M. Niu, 2024). After that, the percentage of malicious IPs was calculated for each selected hosting provider on a monthly basis.

4.3.2. Descriptive summary of the dataset

To better understand the characteristics of the dataset, Figure 4.1 presents the distribution of hosting provider sizes, measured by the total number of IP addresses (Avg_Total_IPs). The histogram reveals that most hosting providers in the dataset operate with a relatively small number of IPs, while a few larger providers manage significantly more. This distribution is highly skewed, with a concentration of small-scale providers and only a few large hosting companies controlling the majority of IPs.

Figure 4.2 presents the distribution of compliance scores among hosting providers, showing how they vary in their adherence to the Digital Services Act (DSA) requirements. The histogram shows that most hosting providers have compliance scores concentrated between 0.3 and 0.6, indicating moderate compliance levels. A smaller number of providers have higher compliance scores (above 0.7), while some have lower compliance levels (below 0.3).

This distribution suggests that full compliance with the DSA is not yet widespread, and many hosting providers fall into the mid-range of regulatory adherence. The absence of strong clustering at high compliance levels implies that providers may face challenges in fully implementing the DSA's requirements. Additionally, the spread of scores highlights that not all providers interpret or apply compliance measures in the same way.

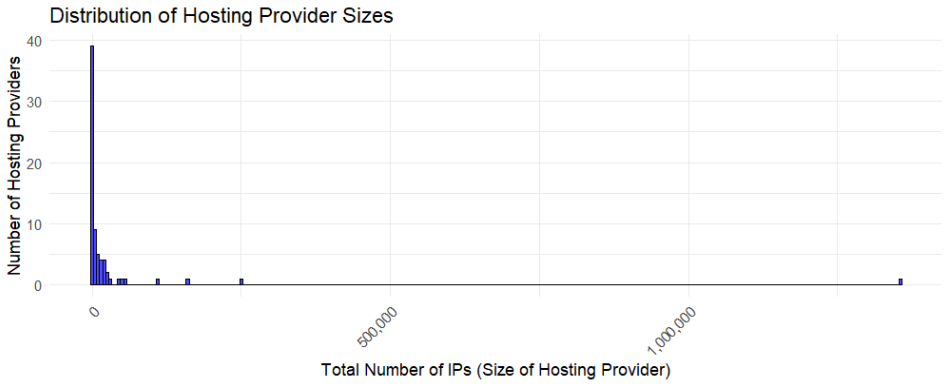

Figure 4.1: Distribution of provider sizes

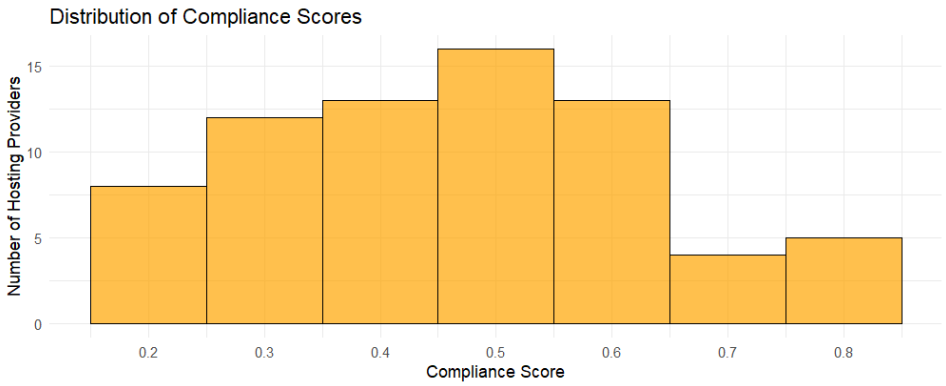

Figure 4.2: Distribution of compliance scores

4.3.3. Analysis of the malicious IP percentages before and after the implementation of the DSA

The analysis was conducted using an Interrupted Time Series (ITS) model to examine the relationship between the implementation of the Digital Services Act (DSA) and the percentage of malicious IP addresses, with a focus on the interaction between time and the DSA implementation period. The ITS model considered three predictors: time, the post-DSA period, and their interaction.

The results are presented in Table 4.1.

Table 4.1: Impact of the DSA on malware percentages

Variable	**Estimate**	**Std. Error**	**t-value**	**p-value**
Intercept	0.0002	0.1678	0.001	0.9990
Time	0.2183	0.1090	2.002	0.0457*
Post_DSA	-0.5029	2.1355	-0.236	0.8139
Time × Post_DSA (Interaction)	0.2140	0.9881	0.217	0.8286
Model Fit				
Residual Std. Error (df = 728)	0.8505			
R^2	0.0084			
Adjusted R^2	0.0043			
F-Statistic (df = 3; 728)	2.044, p = 0.106			

Note: *p < 0.05, **p < 0.01, ***p < 0.001. Standard errors are shown in parentheses.

The regression analysis revealed that the coefficient for the time variable (β = 0.218, p = 0.046) was statistically significant, suggesting a slight upward trend in the percentage of malicious IPs over time, independent of the DSA's implementation. However, the coefficient for the post-DSA intervention (β = -0.503, p = 0.814) was not statistically significant, indicating that there was no immediate reduction in the percentage of malicious IPs after the DSA implementation. Furthermore, the interaction term between time and the post-DSA period (β = 0.214, p = 0.829) was also non-significant, suggesting that the DSA did not have a measurable effect on altering the time-based trajectory of malicious IPs.

These findings are further supported by the visual representation of the ITS analysis, shown in Figure 4.3. The graph shows the percentage of malicious IPs over time, with the red and blue points representing the pre- and post-DSA periods, respectively. A vertical dashed red line marks the implementation of the DSA, while trend lines indicate the linear trajectory of malware percentages before and after the intervention. The pre-DSA period displays a slight upward trend in malware percentages,

consistent with the statistically significant coefficient for the time variable. However, the post-DSA trend remains relatively flat, with no noticeable immediate reduction or significant alteration in trajectory following the DSA's implementation. This graph aligns with the non-significant coefficients for both the post-DSA and interaction terms, further reinforcing the conclusion that the DSA did not significantly impact malicious IP percentages within the observed timeframe.

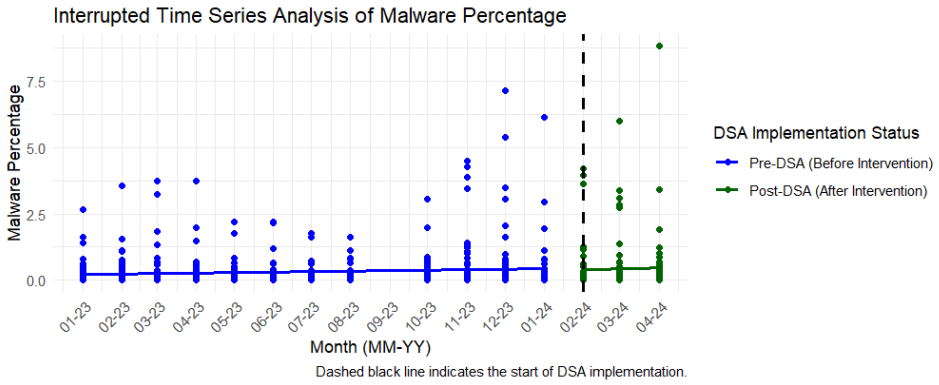

Figure 4.3: Comparison of malicious IP percentages pre-and post DSA

While the results did not provide evidence for a significant immediate or gradual effect of the DSA, the model's residuals displayed heterogeneity, indicating variability across organizations. This could reflect underlying noise in the data or differential responses to the DSA among hosting providers. This observation shows the need to examine how compliance levels and hosting provider characteristics, such as size and focus, interact with malicious activity rates, which will be explored in Section 4.3.3.

Overall, the results suggest that the implementation of the DSA, at least within the observed timeframe and dataset, did not significantly influence the percentage of malicious IPs.

4.3.4. Role of compliance and hosting characteristics in malicious activity rates

This section presents the results of the regression analyses conducted to examine the relationships between compliance score, provider size, client focus, and malware percentage. Seven models in Table 4.2 were tested to investigate the individual effects, combined effects, and interaction effects of these predictors. The findings are detailed below.

Individual effects of compliance score and provider Size

The first two models explored the individual effects of compliance score and provider size on malware percentage.

Model 1 focused on the relationship between compliance score and malware percentage. The regression coefficient for compliance score (β=−0.552,p=0.230) suggested a negative association, where higher compliance scores were associated with lower malware percentages. However, the result was not statistically significant, as the p-value exceeded the conventional threshold of 0.05. The model's R^2 value was 0.021, indicating that compliance score alone explained only 2.1% of the variance in malware percentage. These findings imply that, within the observed dataset, compliance score did not have a strong or reliable influence on malware percentage.

Model 2 examined the effect of provider size, measured by the average total number of IPs (Avg_Total_IPs), on malware percentage. The coefficient for provider size (β=0.000,p=0.983) was close to zero and not

statistically significant, suggesting that provider size had no observable effect on malware percentage. This model had an R^2 value of 0.00001, explaining virtually none of the variation in malware percentage. The lack of significance and explanatory power indicates that provider size, as an individual predictor, does not contribute meaningfully to the observed variability in malware percentage.

Combined effects of compliance score and provider size

Model 3 tested the combined effects of compliance score and provider size on malware percentage. The coefficient for compliance score (β=−0.564,p=0.228) remained similar to the result in Model 1, indicating a consistent but statistically insignificant negative relationship with malware percentage. Provider size (β=0.000,p=0.855) continued to show no significant effect. The R^2 value for this model was 0.021, indicating no improvement in explanatory power compared to Model 1. These results suggest that including provider size alongside compliance score does not improve the model's ability to predict malware percentage.

Interaction between compliance score and provider size

To explore whether provider size moderated the effect of compliance score on malware percentage, Model 4 included an interaction term between compliance score and provider size. The interaction term (β=0.00001,p=0.379) was not statistically significant, indicating no evidence that provider size influenced the relationship between compliance score and malware percentage. The R^2 value increased slightly to 0.033, but this modest improvement in model fit was insufficient to justify the inclusion of the interaction term. These findings suggest that the effect of compliance score on malware percentage operates independently of provider size.

The role of client focus

Model 5 examined the effect of client focus (Public vs. Organization) on malware percentage. The coefficient for client focus (β=0.311,p=0.155) indicated that public providers tend to exhibit higher malware percentages compared to organization-focused providers. However, this result was not statistically significant, as the p-value exceeded 0.05. The model's R^2 value was 0.029, showing that client focus explained 2.9% of the variance in malware percentage. While the direction of the effect aligns with expectations that public-facing providers might be more exposed to abuse, the lack of statistical significance suggests that this relationship is not robust within the observed dataset.

Combined effects of client focus, compliance score, and provider size

Model 6 included all three predictors—client focus, compliance score, and provider size—to examine their combined influence on malware percentage. The coefficient for client focus (β=0.320,p=0.146) was consistent with Model 5, indicating a higher malware percentage for public providers, though the result remained statistically insignificant. Similarly, compliance score (β=−0.583,p=0.210) and provider size (β=0.000,p=0.920) continued to show no significant effects. The R^2 value for this model was 0.052, explaining 5.2% of the variance in malware percentage. The slight increase in R^2 compared to previous models suggests that these variables together provide some explanatory power, but not enough to draw strong conclusions.

Interaction among client focus, compliance score, and provider size

Model 7 incorporated all possible interaction terms among client focus, compliance score, and provider size to explore complex interdependencies. None of the interaction terms, including the three-way interaction (β=0.00002,p=0.903), were statistically significant. The R^2 value for this model was 0.071,

the highest among all models, but the adjusted R^2 was negative (-0.03188), reflecting a poor overall fit. These results indicate that the combined effects of client focus, compliance score, and provider size do not significantly influence malware percentage.

Table 4.2: Regression models for malware percentage

Dependent Variable:	**Malware Percentage**						
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Compliance Score	-0.552		-0.564	-0.684		-0.583	-0.046
	(0.456)		(0.463)	(0.484)		(0.460)	(1.240)
Average Total IPs		0.000	0.000	-0.000		0.000	0.000
		(0.000)	(0.000)	(0.000)		(0.000)	(0.000)
Client Focus (Public)					0.311	0.320	0.733
					(0.216)	(0.217)	(0.685)
Compliance x Size				0.000			-0.000
				(0.000)			(0.000)
Client Focus x Compliance							-0.843
							(1.360)
Client Focus x Size							-0.000
							(0.000)
Client Focus x Compliance x Size							0.00002
							(0.000)
Intercept	0.557*	0.298***	0.559*	0.628*	0.031	0.294	0.040
	(0.226)	(0.078)	(0.228)	(0.242)	(0.201)	(0.289)	(0.625)
Observations	71	71	71	71	71	71	71
R^2	0.021	0.000	0.021	0.033	0.029	0.052	0.071
Adjusted R^2	0.007	-0.014	-0.008	-0.011	0.015	0.009	-0.032
Residual Std. Error	0.637	0.644	0.641	0.642	0.634	0.636	0.649
F Statistic	1.465	0.000	0.739	0.753	2.070	1.223	0.691

*p$<$0.05; **p$<$0.01; ***p$<$0.001. Standard errors in parentheses.

4.4. Implication of the results

The results of this study provide insights into the challenges and complexities of implementing effective regulatory frameworks like the Digital Services Act (DSA) within Dutch hosting providers. While the primary goal of the DSA is to enhance compliance and reduce malicious activity, the findings indicate that its direct impact on malware percentages has been limited. This raises important questions about the practical influence of such policies and offers valuable lessons for policymakers, industry stakeholders, and researchers.

One key insight from the results is the variability in outcomes across hosting providers, which reflects the heterogeneous nature of the industry. Providers differ not only in size but also in their technological capabilities, resource availability, and client focus. While larger firms generally have more resources, such as advanced tools and dedicated cybersecurity teams, this does not automatically translate to lower levels of malware abuse. Larger providers often deal with more complex infrastructures, greater exposure to sophisticated threats, and their scale can make them more attractive targets for malicious actors. On the other hand, smaller providers, although operating with limited resources, might experience less malware abuse due to their reduced visibility or simpler networks, but they remain vulnerable

because they lack robust defenses. While the DSA recognizes these differences and applies differentiated obligations based on provider size, the findings suggest that these measures may not fully address the challenges faced by providers at either end of the spectrum. Both large and small providers encounter unique pressures that require tailored approaches, rather than just relying on size-based categorization.

This is not to suggest that the DSA's framework is inherently flawed. The recognition of industry heterogeneity and the introduction of tiered standards represent a significant step forward in creating fairer regulations. However, the findings indicate a need for further refinement to ensure that these measures translate into meaningful and practical outcomes for all providers. For example, clearer guidance tailored to the specific operational realities of smaller providers could help bridge the gap between regulatory goal and practical implementation. Similarly, providing additional resources, whether financial, technical, or informational, could help smaller providers to comply more effectively and increase the overall impact of the DSA on reducing cyber risks at the same time.

Another important takeaway from these tests is the weak relationship between compliance scores and malware prevalence. This suggests that current compliance metrics may not fully capture the dynamic and multifaceted nature of cybersecurity performance. While compliance frameworks often emphasize adherence to specific technical guidelines, this approach may overlook the operational and real-time challenges faced by providers in preventing and responding to cyber threats. High compliance scores may reflect a provider's ability to meet regulatory checklists, but they do not necessarily guarantee improved security outcomes. This disconnect highlights the need for a shift toward more outcome-oriented measures of compliance. Instead of focusing solely on whether providers meet certain standards, regulators could evaluate the real-world effectiveness of these measures in reducing malicious activity and enhancing cybersecurity resilience.

From a broader perspective, these results emphasize the need for cybersecurity regulations to account for real-world complexities. While the DSA provides a solid foundation, its effectiveness depends on being complemented by practical, collaborative efforts that engage all stakeholders in addressing the challenges of cybersecurity. For instance, partnerships between regulators, hosting providers, and cybersecurity experts could facilitate the sharing of threat intelligence, development of best practices, and creation of joint response strategies.

This chapter explored whether compliance with the Digital Services Act (DSA) has helped Dutch hosting providers reduce malicious activity. The findings suggest that there is no strong evidence that compliance alone leads to a significant drop in malicious IP activity. While the DSA provides a framework for accountability and transparency, the data does not indicate a clear reduction in cyber threats following its implementation.

The Interrupted Time Series (ITS) analysis and regression models revealed that there is only a weak and statistically insignificant correlation between compliance levels and decreases in malicious activity. This suggests that simply following the DSA's requirements does not automatically improve abuse mitigation. Several factors likely influence this outcome, including the ability of cybercriminals to adapt, differences in how hosting providers implement security measures, and challenges in enforcement. Some providers may have strong security practices that go beyond regulatory requirements, while others may comply on paper but struggle to implement effective mitigation strategies.

The results of the analysis highlight the complexity of reducing cyber threats through regulation alone. Although compliance is important, technical solutions, industry cooperation, and enforcement mech-

anisms also play a crucial role. The findings of this chapter lead the discussion further in the next section, where the broader implications of these results will be explored, along with recommendations for improving regulatory effectiveness and security practices.

5

Discussion

This research examined whether compliance with the Digital Services Act (DSA) aids Dutch hosting providers in handling abuse on their networks. By analyzing the relationship between compliance levels and malicious activity, the study assessed how effectively the regulation addresses cyber threats. While the findings suggest that the DSA's impact is not yet statistically significant, comparing these results with existing studies provides important insights into the broader challenges of implementing regulatory frameworks like the DSA.

5.0.1. The complexity of reducing malicious activity Post-DSA

One of the main findings of this research is the lack of a statistically significant reduction in malicious IP percentages after the DSA's implementation. Although the regulation introduced a comprehensive framework, this result reflects the challenges of reducing cybercrime in a dynamic and evolving threat landscape. As (Bendiek, 2021) points out, the rapid evolution of cyber threats often outpaces regulatory measures. His study results also highlight the difficulty of achieving immediate improvements through regulatory interventions alone.

Additionally, the effectiveness of the DSA depends on its gradual adoption by hosting providers, as noted by (G'sell, 2023). Compliance outcomes varied across providers, and the analysis showed no consistent correlation between higher compliance scores and reductions in malicious activity. This variability suggests that meeting compliance requirements procedurally does not always translate into better cybersecurity outcomes. Factors such as the sophistication of cybercriminals and external pressures outside the providers' control likely influence these results. The slight increase in malicious IP percentages observed in the post-DSA dataset could also indicate that certain providers struggle to adapt their operations to meet both the regulatory and technical demands of abuse mitigation.

5.1. Weak correlation between compliance and malware rates

Another key observation is the weak and statistically insignificant correlation between compliance with DSA requirements and reductions in malicious activity. This finding highlights a potential limitation in how compliance is currently measured. As (Gosztonyi et al., 2024) argues, the DSA prioritizes trans-

parency and procedural accountability over direct operational outcomes. This disconnect means that fulfilling compliance requirements does not necessarily guarantee improvements in mitigating abuse.

For example, the DSA mandates notice-and-action mechanisms for handling illegal content. While many providers meet these requirements, this procedural compliance does not always translate into effective abuse detection. Smaller providers may lack the resources to implement robust systems, while larger providers face scalability challenges in managing the volume and complexity of reports. These operational realities help explain the weak correlation observed and suggest that compliance metrics should be complemented by measures that focus on tangible cybersecurity outcomes, such as reductions in successful attacks or response times to abuse reports..

5.2. Reflection of the DSA in practice

This study highlights the complex relationship between compliance with the DSA and anti-abuse practices among Dutch hosting providers. The evaluation of key obligations, such as notice-and-action mechanisms, transparency reporting, and the appointment of legal representatives, shows that adherence to the DSA alone may not lead to significant improvements in mitigating malicious activity. This raises important questions about how the DSA is implemented and its ability to address the challenges providers face, particularly those with different operational focuses, such as public-facing or enterprise-focused services. While the DSA provides a valuable regulatory framework, its impact may depend on complementary measures, such as advanced technical solutions or industry-wide collaboration, to achieve its intended goals.

5.3. Roles in abuse mitigation

While hosting providers may play a critical role in detecting and mitigating abuse, they do not operate alone. Effective abuse mitigation requires collaboration among multiple stakeholders; each one of them contributes in different ways to detect, monitor, and prevent abuse. These stakeholders include law enforcement agencies, regulatory bodies, security professionals, and end users, whom all influence how abuse is addressed within hosting society.

Hosting providers act as the first line of defense, monitoring network activity, blocking malicious IPs, and responding to abuse reports. However, their effectiveness is often limited by resource constraints, weak enforcement policies, and jurisdictional challenges. When abuse involves criminal activity or large-scale fraud, law enforcement agencies step in to investigate and take legal action, but cross-border cybercrime and slow legal processes often hinder timely intervention. Regulatory bodies, such as the European Commission and national cybersecurity agencies, set compliance standards like the Digital Services Act (DSA), but inconsistent enforcement can reduce their effectiveness. Security professionals and threat intelligence platforms provide valuable insights by tracking and reporting malicious activity, yet their impact relies on voluntary cooperation from hosting providers, who may not always act on external intelligence. Meanwhile, end users, including businesses and individual victims, contribute by reporting phishing, malware, and abuse, but underreporting and slow response times weaken the effectiveness of user-driven defense efforts. The interaction among these stakeholders creates both strengths and weaknesses in how abuse is controlled. This shows that simply following the DSA rules is not enough to fully prevent and reduce cyber threats. Instead, a joint effort is needed, where law enforcement, regulators, security professionals, and the end users work together.

5.4. Broader implications of the findings

The findings have broader implications for both policymakers and hosting providers. For policymakers, they highlight the need for regulatory frameworks to evolve alongside emerging threats. As (Bendiek, 2021) notes, the DSA's long-term success depends on its adaptability. The weak correlation between compliance and malware rates observed in this study suggests that compliance metrics should emphasize tangible outcomes, such as reductions in abuse incidents, rather than procedural adherence alone. Policymakers could also consider incentivizing the adoption of advanced cybersecurity measures, such as enhanced threat detection systems and improved incident response protocols.

For hosting providers, the persistence of malicious activity despite regulatory interventions underscores the need to integrate compliance with proactive security practices. Providers must invest in advanced detection tools, robust incident response capabilities, and staff training to effectively manage abuse. Collaboration within the industry, such as sharing threat intelligence and best practices, could also strengthen collective resilience. These findings show that while the DSA may offer a baseline framework, its effectiveness ultimately depends on the proactive efforts of hosting providers and their ability to address the realities of cyber threats.

5.5. Reflection on the methodology

The methodology for this study was developed to investigate the impact of the Digital Services Act (DSA) on malicious activity and the compliance practices of Dutch hosting providers. The research relied on Interrupted Time Series (ITS) analysis to measure changes in malicious IP percentages before and after the implementation of the DSA. This method was chosen because it can track changes over time while considering patterns that were already present in the data before the time DSA was implemented. However, ITS is most reliable when at least 12 time points before and 12 time points after the intervention are available. Due to data limitations, this study did not fully meet this recommendation, which may impact the reliability of segmented regression estimates. A shorter time series increases the risk that observed changes are due to short-term fluctuations rather than a lasting impact of the DSA. Future research could address this by extending the observation period, allowing for a more comprehensive analysis of long-term trends and reducing the risk of misinterpreting short-term fluctuations as regulatory effects.

To complement this, regression models were used to explore the relationship between compliance levels and malicious activity, providing further insights into how hosting providers' adherence to the DSA's requirements relates to their ability to mitigate abuse. While this approach allowed for structured evaluation, the study relied on a single dataset for both calibration and validation, meaning that model predictions were not tested on unseen data. A more rigorous approach could involve splitting the dataset into anaylsis and validation subsets, allowing for a better assessment of how well the model generalizes beyond the observed sample. Additionally, the regression model treated all hosting providers as independent observations, which may not fully capture provider-specific differences in compliance behavior. A mixed-effects model, where hosting providers are treated as random effects while compliance levels and other variables remain fixed, could provide a more refined understanding of variations in compliance impact across different types of providers. Future studies could benefit from incorporating these adjustments to improve model robustness.

A key strength of the methodology was its ability to provide a structured evaluation of the DSA's effectiveness. ITS analysis allowed for a clear comparison of malicious activity over time, identifying

potential changes associated with the regulation. By controlling for pre-existing trends, the study ensured that any observed changes could be more confidently linked to the DSA rather than unrelated external factors. Regression models added another layer of depth, helping to identify whether higher compliance scores related with DSA translated into measurable reductions in malicious activity. These combined approaches offered a robust framework for assessing both the direct and indirect effects of the regulation.

The alignment between this study's findings and the broader literature further strengthens the validity of the research framework. As (Gosztonyi et al., 2024) explains, the DSA's monitoring obligations limit the scope of regulatory oversight, aiming to balance governance with fundamental rights. While this balance is important, it also makes reducing malicious activity through regulations alone more difficult. The findings of this study highlight this complexity, showing that the persistence of abuse is not a shortcoming of the DSA but rather a reflection of the diverse challenges it addresses.

Defining the key terms, such as "hosting providers" and "malicious IPs" also providers clarity to the study.By focusing on Dutch hosting providers and excluding non-relevant entities like CDNs, the analysis stayed aligned with the DSA's intended scope. Malicious activity was identified using threat intelligence data from sources like Spamhaus, which, while widely used in the industry, has its limitations in terms of comprehensiveness and accuracy. Nevertheless, it provided a practical and consistent basis for measuring abuse, ensuring the findings remained relevant to the research objectives while avoiding unnecessary ambiguity.

5.6. Limitations and challenges

While this research provides insights into the impact of the Digital Services Act (DSA) on malicious activity and compliance practices among Dutch hosting providers, several limitations must be acknowledged. These limitations reflect challenges in data availability, scope, and the broader complexities of regulatory evaluation.

One of the primary limitations is the relatively short timeframe for analysis. The DSA has not been in effect for long, and regulatory impacts, particularly in the context of cybersecurity, often require extended periods to materialize. Hosting providers need time to adapt their internal policies, implement compliance measures, and adjust operational practices, meaning that any reduction in malicious activity may not be immediately visible. Additionally, changes in cybercriminal behavior, enforcement measures, and external regulatory pressures may take longer to influence measurable trends. Expanding the analysis to include a longer post-implementation period would allow for a more thorough evaluation of the DSA's long-term effects, reducing the risk of misattributing short-term fluctuations to the regulation itself.

Another significant limitation lies in the small size of the dataset, which makes it difficult to draw strong conclusions regarding trends or the absence of trends. With a limited number of observations, particularly for post-DSA implementation, it becomes more challenging to distinguish meaningful changes from statistical noise. Small datasets increase the likelihood of random variability influencing results, making it harder to detect whether any observed changes are due to the intervention or simply due to fluctuations in the data. A larger dataset—either by including more providers, extending the timeframe, or integrating additional threat intelligence sources would improve the reliability of trend analyses and provide a better statistical foundation for evaluating the DSA's impact.

Furthermore, intervention effects may not be immediate, meaning that a delayed response to the DSA's implementation could impact the results. While ITS analysis assumes that changes occur relatively soon after an intervention, policy-driven shifts often take longer to manifest. Hosting providers may require months to adjust internal policies, refine abuse mitigation strategies, and respond to new regulatory requirements. Additionally, cybercriminals may alter their attack methods over time, leading to delayed fluctuations in malicious activity. This means that a change in the trend of malicious activity might not be observed immediately after the DSA's implementation but could emerge over multiple time periods. Future research should consider methodologies that account for delayed intervention effects, such as lagged regression models or extended observation periods, to better capture the full impact of regulatory interventions.

While this study derived measurable requirements from the DSA, the regulation itself has not yet been fully translated into practical guidelines by the European Commission. As a result, hosting providers lack a standardized compliance framework, making it difficult to determine whether their efforts align with regulatory expectations. This ambiguity affects the ability to assess the practical effectiveness of compliance measures, as different providers may interpret and implement compliance differently. Incorporating alternative compliance assessment methods, such as direct engagement with hosting providers or tracking enforcement actions, could improve the accuracy of compliance measurements.

The study's focus on Dutch hosting providers, while necessary for maintaining a manageable scope, also narrows the generalizability of its findings. The regulatory environment and market dynamics in the Netherlands may differ from those in other jurisdictions. For instance, the enforcement of the DSA in the Netherlands may vary in strictness compared to other EU member states. This makes it challenging to evaluate whether observed trends are unique to the Dutch context or indicative of broader patterns across Europe. Comparative studies cover multiple jurisdictions could provide a more comprehensive understanding of the DSA's effectiveness.

Data limitations also posed a challenge. The reliance on publicly available data, while practical, may not fully capture the complexity of compliance or the operational realities of hosting providers. Additionally, this study did not include perspectives from law enforcement, auditors, or industry professionals who are directly involved in implementing and enforcing the DSA. Their insights could provide valuable context on how well the regulation is being enforced and whether companies face specific challenges in translating its requirements into actionable practices.

5.7. Future research recommendations

This study highlights several areas where future research could build upon the findings and address the limitations encountered. Expanding the scope and methods of analysis would provide a more comprehensive understanding of the Digital Services Act (DSA) and its impact on compliance and cybersecurity practices.

First, extending the observation period to include more data from the years following the DSA's implementation would help capture its long-term effects. Regulatory changes often take time to fully influence industry practices, and a longer timeframe would allow researchers to better assess trends and identify whether the DSA leads to lasting reductions in malicious activity.

One key area for future research is extending the observation period to include a longer post-implementation timeframe. Regulatory changes such as the DSA do not always produce immediate effects, as hosting

providers require time to adjust their compliance strategies, implement technical mitigation measures, and respond to enforcement actions. Additionally, cybercriminals may modify their tactics in response to increased enforcement, causing delayed shifts in malicious activity trends. A longer dataset would allow researchers to determine whether observed changes are temporary fluctuations or part of a sustained trend, helping to assess the true long-term impact of the DSA on abuse mitigation.

Second, future research could explore the DSA's impact across multiple jurisdictions rather than focusing solely on Dutch hosting providers. Comparing countries with different enforcement practices and regulatory environments would provide valuable insights into how local factors influence compliance and effectiveness. Such studies could also highlight whether the findings in this research are unique to the Netherlands or reflective of broader trends across the EU.

Improvements in statistical modeling techniques would also strengthen future studies on the DSA's impact. Segmented regression in ITS analysis is most effective when at least 12 pre- and post-intervention time points are available, but this study had a shorter timeframe, which may have influenced the results. Extending the number of observation points would improve statistical robustness, allowing for a more reliable analysis of policy effects and reducing the impact of short-term fluctuations in the data. Additionally, incorporating mixed-effects regression models, where hosting providers are treated as random effects, would allow for better control of provider-specific variations in compliance behavior. Model validation could also be improved by splitting the dataset into training and validation subsets, ensuring that predictive models are tested on unseen data and not overly dependent on the existing sample.

Additionally, future studies could incorporate qualitative methods, such as interviews or surveys, to gather insights from law enforcement agencies, auditors, and industry professionals. These perspectives would provide a deeper understanding of how the DSA is enforced in practice and the challenges companies face in implementing its requirements. It would also be valuable to consider case studies that examine whether compliance with the DSA has led to measurable improvements in reducing abuse within specific hosting providers' networks.

Finally, future studies should take the role of external factors into consideration, such as the increasing sophistication of cybercriminals, geopolitical tensions, or the introduction of other regulations, in shaping trends in malicious activity. Geopolitical conflicts can influence cybercrime dynamics, with state-sponsored actors or politically motivated attacks potentially increasing the prevalence of malicious activity.

6

Conclusion

This research aimed to examine the impact of the Digital Services Act (DSA) on malicious activity among Dutch hosting providers, evaluating whether compliance with the regulation translates into improved cybersecurity outcomes. The findings suggest that while the DSA establishes a structured compliance framework, its immediate effects on reducing cyber threats remain unclear. The analysis showed no statistically significant reduction in malicious IP activity post-DSA implementation, highlighting the challenges of regulatory interventions in a constantly evolving cyber threat landscape. This aligns with existing research indicating that cyber threats often adapt faster than policy measures, making it difficult to observe immediate security improvements solely through compliance requirements.

A key finding from this study is the weak correlation between compliance and reductions in malware rates. While transparency, accountability, and procedural adherence are central to the DSA, they do not automatically result in enhanced abuse mitigation. Hosting providers vary widely in their technical capabilities, resource allocation, and enforcement of security practices, meaning that compliance alone does not necessarily equate to stronger cybersecurity measures. The findings suggest that regulatory frameworks need to be supplemented by technical enforcement mechanisms, industry collaboration, and proactive security measures to achieve tangible improvements in abuse prevention.

Another important insight from this research is that abuse mitigation is not the sole responsibility of hosting providers. Law enforcement agencies, regulatory bodies, security professionals, and end users all play a role in addressing cyber threats, yet their interactions and coordination remain inconsistent. The study highlights gaps in enforcement and cooperation, showing that simply following compliance guidelines does not address the root causes of abuse. Hosting providers operate within a broader cybersecurity ecosystem, where delays in enforcement, jurisdictional challenges, and resource constraints all influence the effectiveness of abuse mitigation efforts.

Moreover, this research emphasizes methodological and data-related limitations that should be considered in future studies. The short observation period may not fully capture the long-term impact of the DSA, as regulatory interventions often take time to produce measurable changes. Additionally, the small dataset limits the ability to draw definitive conclusions about broader trends. The study also acknowledges that compliance scoring methods may not fully reflect real-world enforcement efforts,

suggesting the need for alternative approaches to assessing provider accountability and security effectiveness. Future research should consider longer timeframes, comparative analyses across different geolocations, and mixed-method approaches that incorporate both quantitative and qualitative insights to better assess the effectiveness of cybersecurity regulations like the DSA.

Finally, the study reviews role of regulations in cybersecurity, reinforcing the idea that policy alone is not sufficient to mitigate online threats. While the DSA provides an important legal and procedural framework, its effectiveness depends on complementary measures, including technological advancements, stronger enforcement mechanisms, and improved industry collaboration. As cyber threats continue to evolve, regulatory approaches must be adaptive, data-driven, and supported by proactive security measures to provide a safer online environment.

References

Akella, S. R., Vydula, D. L., Ozer, M., Kose, Y., Bastug, M., Onat, I., Elsayed, N., ElSayed, Z., & Koseli, M. (2023). Understanding cyber threats: Patterns, isp characteristics, industry targets, and geographic correlations. *2023 International Conference on Computational Science and Computational Intelligence (CSCI)*, 811–815. https://doi.org/10.1109/CSCI62032.2023.00137

Akinsanya, M. O., Ekechi, C. C., & Okeke, C. D. (2024). The evolution of cyber resilience frameworks in network security: A conceptual analysis. *Computer Science & IT Research Journal*, *5*(4), 926–949.

Alkemade, G., & Toet, J. (2021). Data protection regulation in the netherlands. *Data Protection Around the World: Privacy Laws in Action*, 165–188.

Alrwais, S., Liao, X., Mi, X., Wang, P., Wang, X., Qian, F., Beyah, R., & McCoy, D. (2017). Under the shadow of sunshine: Understanding and detecting bulletproof hosting on legitimate service provider networks. *2017 IEEE Symposium on Security and Privacy (SP)*, 805–823. https://doi.org/10.1109/SP.2017.32

Antonakakis, M., Perdisci, R., Lee, W., Vasiloglou, N., & Dagon, D. (2011). Detecting malware domains at the upper dns hierarchy, 27–27.

Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The role of machine learning in cybersecurity. *Digital Threats*, *4*(1). https://doi.org/10.1145/3545574

Bendiek, A. (2021). The impact of the digital service act (dsa) and digital markets act (dma) on european integration policy. *Working Paper Research Division EU/Europe 2021*, (02), 15.

Bilge, L., Sen, S., Balzarotti, D., Kirda, E., & Kruegel, C. (2014). Exposure: A passive dns analysis service to detect and report malicious domains. *ACM Trans. Inf. Syst. Secur.*, *16*(4). https://doi.org/10.1145/2584679

Canali, D., Balzarotti, D., & Francillon, A. (2013). The role of web hosting providers in detecting compromised websites. *Proceedings of the 22nd International Conference on World Wide Web*, 177–188. https://doi.org/10.1145/2488388.2488405

Chang, J., Venkatasubramanian, K. K., West, A. G., & Lee, I. (2013). Analyzing and defending against web-based malware. *ACM Comput. Surv.*, *45*(4). https://doi.org/10.1145/2501654.2501663

Chen, L., Zhang, Y., Zhao, Q., Geng, G., & Yan, Z. (2018). Detection of dns ddos attacks with random forest algorithm on spark [The 15th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2018) / The 13th International Conference on Future Networks and Communications (FNC-2018) / Affiliated Workshops]. *Procedia Computer Science*, *134*, 310–315. https://doi.org/https://doi.org/10.1016/j.procs.2018.07.177

Eeten, M., Bauer, J., Asghari, H., Tabatabaie, S., & Rand, D. (2010). The role of internet service providers in botnet mitigation: An empirical analysis based on spam data. *Journal Name*, 123–145.

European Commission. (2022, November). Digital services act: Eu's landmark rules for online platforms enter into force [Press release IP/22/6906]. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6906

European Parliament and Council of the European Union. (2022). Regulation (eu) 2022/2065 of the european parliament and of the council of 19 october 2022 on a single market for digital services and amending directive 2000/31/ec (digital services act) [Text with EEA relevance]. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065

Forum, W. E. (2023). Global cybersecurity outlook 2023: Cybercrime and system safety [Available at https://www.weforum.org/stories/2024/01/cybersecurity-cybercrime-system-safety/].

Fryer, H., Stalla-Bourdillon, S., & Chown, T. (2015). Malicious web pages: What if hosting providers could actually do something… *Computer Law and Security Review*, *31*(4), 490–505. https://doi.org/https://doi.org/10.1016/j.clsr.2015.05.011

Geer, D., Jardine, E., & Leverett, E. (2020). On market concentration and cybersecurity risk. *Journal of Cyber Policy*, *5*(1), 9–29.

Gosztonyi, G., Galewska, E., & Školkay, A. (2024). Challenges of monitoring obligations in the european union's digital services act. *ELTE Law Journal*, (1), 45–60.

Greitzer, F., & Hohimer, R. (2011). Modeling human behavior to anticipate insider attacks. *Journal of Strategic Security*, *4*, 194–202. https://doi.org/10.5038/1944-0472.4.2.2

G'sell, F. (2023). The digital services act (dsa): A general assessment. *Content Regulation in the European Union–The Digital Services Act, TRIER STUDIES ON DIGITAL LAW*, *1*.

Hernandez-Suarez, A., Sanchez-Perez, G., Toscano-Medina, L. K., Olivares-Mercado, J., Portillo-Portilo, J., Avalos, J.-G., & Garcia Villalba, L. J. (2022). Detecting cryptojacking web threats: An approach with autoencoders and deep dense neural networks. *Applied Sciences*, *12*(7), 3234.

Husovec, M., & Roche Laguna, I. (2022). Digital services act: A short primer. *Martin Husovec and Irene Roche Laguna, Principles of the Digital Services Act (Oxford University Press, Forthcoming 2023)*.

Hyder, M. F., Ahmed, W., & Ahmed, M. (2022). Toward deceiving the intrusion attacks in containerized cloud environment using virtual private cloud□based moving target defense. *Concurrency and Computation: Practice and Experience*, *35*. https://doi.org/10.1002/cpe.7549

Hynek, K., Vekshin, D., Luxemburk, J., Cejka, T., & Wasicek, A. (2022). Summary of dns over https abuse. *IEEE Access*, *10*, 1–1. https://doi.org/10.1109/ACCESS.2022.3175497

Jyothi, A., Mallika, C., Jahnavi, V., Naga, C., Varma, A., Shekar, K., & Nirmal, C. (2024). Unmasking phishing threats through cutting-edge machine learning. *International Journal of Innovative Science and Research Technology (IJISRT)*, 1359–1366. https://doi.org/10.38124/ijisrt/IJISRT24APR1022

Kamara, I., Leenes, R., Stuurman, C., & Van den Boom, J. (2020). The cybersecurity certification landscape in the netherlands after the union cybersecurity act.

Kazim, M., & Evans, D. (2016). Threat modeling for services in cloud. *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 66–72. https://doi.org/10.1109/SOSE.2016.55

Kshetri, N. (2010). Cloud computing in developing economies. *IEEE Computer*, *43*(10), 47–55.

Loos, M. (2021). The (proposed) transposition of the digital content directive in the netherlands. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, *12*, 229.

Lu, D., Fei, J., & Liu, L. (2023). A semantic learning-based sql injection attack detection technology. *Electronics*, *12*(6). https://doi.org/10.3390/electronics12061344

Mirheidari, S. A., Arshad, S., Khoshkdahan, S., & Jalili, R. (2012). Two novel server-side attacks against log file in shared web hosting servers. *2012 International Conference for Internet Technology and Secured Transactions*, 318–323.

Mueller, M. L. (2010). *Networks and states: The global politics of internet governance*. MIT Press.

Muir, J. A., & Oorschot, P. C. V. (2009). Internet geolocation: Evasion and counterevasion. *Acm computing surveys (csur)*, *42*(1), 1–23.

Niu, M. (2024). Code for dsa compliance and malicious ip analysis. https://doi.org/10.5281/zenodo.14879682

Niu, W., Li, T., Zhang, X., Hu, T., Jiang, T., & Wu, H. (2019). Using xgboost to discover infected hosts based on http traffic. *Security and Communication Networks*, *2019*(1), 2182615.

Pereira, M. (2021). Taming europe's digital landscape? brief notes on the proposal for a digital services act. *UNIO–EU Law Journal*, *7*(2), 77–94.

Quintais, J. P., & Schwemer, S. F. (2022). The interplay between the digital services act and sector regulation: How special is copyright? *European Journal of Risk Regulation*, *13*(2), 191–217.

Rajasekharaiah, K. M., Dule, C. S., & Sudarshan, E. (2020). Cyber security challenges and its emerging trends on latest technologies. *IOP Conference Series: Materials Science and Engineering*, *981*(2), 022062. https://doi.org/10.1088/1757-899X/981/2/022062

Statista. (2023). Number of malware attacks worldwide from 2015 to 2023 [Available at https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/].

Tajalizadehkhoob, S., Gañán, C., Noroozian, A., & Eeten, M. v. (2017). The role of hosting providers in fighting command and control infrastructure of financial malware. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 575–586.

Tajalizadehkhoob, S., Korczyński, M., Noroozian, A., Gañán, C., & van Eeten, M. (2016). Apples, oranges and hosting providers: Heterogeneity and security in the hosting market. *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, 289–297. https://doi.org/10.1109/NOMS.2016.7502824

Tasnim, R., Mim, A. A., Mim, S. H., & Jabiullah, M. I. (2022). A comparative study on three selective cloud providers. *arXiv preprint arXiv:2208.14482*.

Turillazzi, A., Taddeo, M., Floridi, L., & Casolari, F. (2023). The digital services act: An analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, *15*(1), 83–106.

Vasek, M., Weeden, M., & Moore, T. (2016). Measuring the impact of sharing abuse data with web hosting providers. *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, 71–80.

Ventures, C. (2021). Cybersecurity ventures predicts global cybercrime costs to grow by 15% per year over the next five years, reaching $10.5 trillion usd annually by 2025 [Accessed: 2024-08-26].

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security [Cybercrime in the Digital Economy]. *Computers and Security*, *38*, 97–102. https://doi.org/https://doi.org/10.1016/j.cose.2013.04.004

Wilman, F., Kalėda, S. L., & Loewenthal, P.-J. (2024). *The eu digital services act*. Oxford University Press.

Zhou, C. V., Leckie, C., Karunasekera, S., & Peng, T. (2008). A self-healing, self-protecting collaborative intrusion detection architecture to trace-back fast-flux phishing domains. *NOMS Workshops 2008 - IEEE Network Operations and Management Symposium Workshops*, 321–327. https://doi.org/10.1109/NOMSW.2007.50

A

List of hosting providers

The following is the list of hosting providers identified based on the filtering process described in the methodology:

- AltusHost
- AltusHost B.V.
- BlackHOST Ltd.
- Clouvider Limited
- Global Layer
- IncogNET
- NFOrce Entertainment B.V.
- Apeiron Global
- Asimo Networks
- Dream Vps
- Hoasted
- Hoasted B.V.
- HostRound LLC
- Intermax Group
- LeaseWeb Network
- LeaseWeb Network B.V.
- ProcoliX
- Steadcloud
- True B.V.
- CLDIN B.V.

- Greenhost BV
- HostSlim
- Itglobal.com Nl
- MOJOHOST
- Nextpertise B.V.
- Prolocation BV
- Zomro
- BIT
- BIT BV
- BitCommand
- BlueVPS OU
- CJ2 Hosting B.V.
- Combell
- Combell NV
- CrownCloud
- DC Host
- Deft Hosting
- Digital Ocean
- Dream Vps Ltd
- Duocast B.V.
- EUROHOSTER
- GoodLeaf Hosting & Development
- Greenhost
- Host Europe
- Host Sailor Ltd
- HostHatch, Inc
- HostPalace Web Solution PVT LTD
- HostSlim B.V.
- Hostinger International
- Hostinger International Limited
- Hostkey
- Hostline, Uab
- Hydra Communications
- Hydra Communications Ltd
- Interkvm Host Srl
- KnownSRV

- LeaseWeb Netherlands B.V.
- MIRhosting
- Mojohost B.v.
- Mullvad VPN
- One.com A/S
- PEACEWEB
- Pocos
- Pq Hosting S.r.l.
- RoyaleHosting
- Serverpoint
- SpectraIP
- UpCloud Ltd
- Webzilla
- Zomro B.V.
- xTom