From Anti-Piracy to Cybersecurity: Leveraging Website Blocking in an Integrated Digital Ecosystem

Aaron Herps , Paul A. Watters * , Daniela Simone , Jeffrey Foster

Posted Date: 24 December 2024

doi: 10.20944/preprints202412.1983.v1

Keywords: Piracy; Website blocking; Cybersecurity; Threat Intelligence; Quasi-experimental Methods

Article

From Anti-Piracy to Cybersecurity: Leveraging Website Blocking in an Integrated Digital Ecosystem

Aaron Herps [1], Paul A. Watters [2*], Daniela Simone [3] and Jeffrey Foster [4]

[1] Macquarie University; aaron.herps@hdr.mq.edu.au
[2] Cyberstronomy Pty Ltd; ceo@cyberstronomy.com
[3] Macquarie University; daniela.simone@mq.edu.au
[4] Macquarie University; jeff.foster@mq.edu.au
* Correspondence: ceo@cyberstronomy.com

Abstract: This study evaluates the effectiveness of website blocking as a cybersecurity control to mitigate copyright infringement, focusing on Southeast Asia's diverse legal and technological environments. Using a quasi-experimental design during the COVID-19 pandemic, this research examines the impact of website blocking measures in Indonesia, Vietnam, Malaysia, and Singapore. For the first time, the findings reveal that swift, systematic website blocking—exemplified by Indonesia—serves as an effective cybersecurity control, significantly reducing access to infringing content while redirecting traffic toward legitimate platforms. Jurisdictions with procedural delays and inconsistent enforcement, however, demonstrate limited efficacy, highlighting the need for dynamic responses to evolving threats such as domain hopping and proxy servers. The findings inform broader cybersecurity applications like network segmentation, access control, and threat intelligence. This work links traditional copyright enforcement to proactive incident detection and response strategies, providing insights into broader applications for cybersecurity, such as network segmentation, access control, and threat intelligence.

Keywords: Piracy; Website blocking; Cybersecurity; Threat Intelligence; Quasi-experimental Methods

1. Introduction

The rapid proliferation of digital technologies and the internet has dramatically transformed the global content creation, distribution, and consumption landscape. These technological advances have democratized access to information and entertainment, empowering creators and audiences alike. However, they have also facilitated the rise of pervasive online copyright infringement, presenting a formidable challenge for governments, rights holders, and law enforcement agencies worldwide [1]. This dual-edged nature of digital transformation underscores the urgent need for effective, adaptive strategies to combat online piracy, particularly in regions like Southeast Asia, where the digital ecosystem is evolving rapidly, and cybersecurity risks are growing as a result of piracy[2].

Website blocking has emerged as one of the most prominent tools in the fight against online piracy [3]. At its core, website blocking seeks to restrict access to infringing content by targeting websites that facilitate copyright violations [4]. Implemented at the network level, this approach enables internet service providers (ISPs) to prevent users from accessing specific URLs or domains associated with piracy [5]. This mechanism, while conceptually straightforward, is rooted in complex legal, technological, and procedural frameworks that vary significantly across jurisdictions [6]. Southeast Asia presents a compelling case study for evaluating website blocking measures, given the region's diverse legal systems, varied enforcement mechanisms, and rapidly growing digital economies [7].

 doi:10.20944/preprints202412.1983.v1

Despite its increasing adoption, website blocking as a strategy is not without controversy. Advocates highlight its potential to reduce piracy traffic, redirect users toward legitimate content platforms, and disrupt the financial incentives that drive piracy networks [8]. However, critics point to concerns over the potential for overblocking, where legitimate websites are inadvertently targeted, and the circumvention tactics employed by piracy operators, such as domain hopping and proxy servers, which can undermine blocking efforts [9]. These challenges raise critical questions about the effectiveness and sustainability of website blocking as an anti-piracy measure [10].

Moreover, the global COVID-19 pandemic further complicated the online piracy landscape and the role of blocking [11]. Lockdowns and social distancing measures prompted a dramatic surge in digital content consumption, creating new opportunities for both legal platforms and piracy operators – and new cyber threats [12]. The closure of cinemas, live entertainment venues, and other traditional content distribution channels drove audiences online, amplifying the demand for digital content [13]. While this shift benefited streaming services and legal content providers, it also expanded the market for infringing content, highlighting the urgent need for robust anti-piracy strategies. This unique context provides a valuable natural experiment for evaluating the effectiveness of website blocking measures under extraordinary societal conditions[1].

1.1. Website Blocking in the Southeast Asian Context

Southeast Asia is a particularly relevant region for studying the implementation and impact of website blocking. The region's rapid digital transformation has positioned it as a hotspot for both legitimate and pirated content consumption. According to industry reports, Southeast Asia is home to some of the world's most active internet users, with a significant portion of digital activity centred around media consumption. However, this digital growth has also made the region a focal point for piracy networks, which exploit the region's fragmented regulatory landscape to distribute infringing content.

The legal and enforcement frameworks governing website blocking in Southeast Asia vary significantly between countries, reflecting differences in political priorities, institutional capacities, and levels of stakeholder engagement. Indonesia and Vietnam, for instance, have adopted administrative-based approaches to website blocking, allowing government agencies to swiftly issue blocking orders without requiring judicial oversight. In contrast, Malaysia and Singapore rely on more formalized legal procedures, emphasizing judicial review and due process. These distinctions provide a unique opportunity to analyze how different legal frameworks influence the effectiveness of website blocking measures.

Furthermore, the socio-cultural context of Southeast Asia adds another layer of complexity. The region's diverse linguistic and cultural landscape influences content preferences and piracy behavior, with local and regional piracy networks catering to specific market segments. This diversity underscores the need for tailored anti-piracy strategies that account for local nuances while addressing the broader challenges of digital piracy.

1.2. The Broader Role of Website Blocking in Cybersecurity

While website blocking is traditionally viewed as an anti-piracy tool, this study situates it within the broader context of cybersecurity. At its core, website blocking shares fundamental principles with cybersecurity measures designed to restrict access to malicious or harmful online content [15]. Similar to how firewalls and network filters prevent unauthorized access to sensitive systems, website blocking seeks to disrupt access to infringing content, thereby mitigating the harm caused by piracy [16].

This alignment with cybersecurity principles is particularly relevant in an era defined by the convergence of cybersecurity, artificial intelligence (AI), and IoT technologies [17]. As digital ecosystems become increasingly interconnected, the lines between content protection, data security, and network integrity are blurring. Website blocking, when integrated with advanced cybersecurity

[1] For further details regarding quasi-experimental designs, see a review in [14].

 doi:10.20944/preprints202412.1983.v1

technologies such as AI-driven threat detection and real-time monitoring, has the potential to evolve into a more dynamic and adaptive control mechanism [18]. This expanded perspective opens new avenues for leveraging website blocking beyond copyright enforcement, addressing broader challenges such as phishing, malware distribution, and other forms of cybercrime, where AI is proving to be effective in incident response and deterrence [19].

1.3. Research Significance and Objectives

This study aims to contribute to the ongoing discourse on the effectiveness of website blocking by providing an empirical analysis of its implementation in four Southeast Asian countries: Indonesia, Vietnam, Malaysia, and Singapore. These countries were selected based on their distinct legal frameworks, enforcement practices, and representativeness of the broader region. By examining the impact of website blocking across these diverse jurisdictions, this research seeks to address two critical questions:

1. How do legal frameworks and practical implementations of website blocking measures influence their effectiveness in reducing online copyright infringement?
2. To what extent are website blocking measures effective, and what factors contribute to their success or limitations?

Ultimately, this research aims to provide actionable insights for policymakers, rights holders, and cybersecurity professionals seeking to develop more effective and sustainable strategies for combating online piracy and enhancing digital resilience. By bridging the gap between traditional copyright enforcement and modern cybersecurity practices, this study contributes to a more integrated approach to addressing the challenges of the digital age.

2. Materials and Methods

This study employs a quasi-experimental design to evaluate the effectiveness of website blocking as a cybersecurity measure against online piracy. The COVID-19 pandemic created a unique natural experiment setting, characterized by unprecedented changes in internet usage patterns, enforcement priorities, and content consumption behaviors. These factors allow for a detailed and opportunistic analysis of the implementation and impact of website blocking measures in four Southeast Asian jurisdictions: Indonesia, Vietnam, Malaysia, and Singapore.

2.1. Study Design

To assess the effectiveness of website blocking, this study compares piracy traffic patterns and enforcement outcomes in these jurisdictions with two control territories, Thailand and the Philippines, where no comprehensive website blocking measures were implemented during the study period. The inclusion of control territories enables the isolation of blocking measures' impact from broader trends in digital content consumption, providing a robust basis for comparison.

The design includes two main phases:

1. **Comparative Analysis**: Evaluates differences in piracy levels, implementation efficiency, and legal frameworks across the four target jurisdictions

2. Empirical Measurement: Assesses the quantitative impact of website blocking on piracy traffic and legal content consumption using statistical methods, including raw data analysis, normalized comparisons, and regression modeling.

2.2. Grouping and Selection of Jurisdictions

The selection of Indonesia, Vietnam, Malaysia, and Singapore as the focus of this study reflects the diversity of legal frameworks and practical approaches to website blocking in Southeast Asia. These jurisdictions represent distinct enforcement paradigms, ranging from administrative-based processes to judicially intensive frameworks. They are grouped as follows:

Group 1: Indonesia and Vietnam

1. Characterized by administrative approaches to website blocking.

 doi:10.20944/preprints202412.1983.v1

2. Implementations occur rapidly, often within 24 hours (Indonesia) or a few days (Vietnam).
3. Judicial oversight is minimal or absent, allowing for streamlined decision-making.

Group 2: Malaysia and Singapore

1. Defined by formal legal procedures, emphasizing judicial or quasi-judicial reviews.
2. Implementation timelines are longer, ranging from 48 hours (Malaysia) to several months (Singapore).
3. Blocking orders require extensive documentation and legal scrutiny.

Control Territories

Thailand and the Philippines serve as baselines, as they did not implement systematic website blocking during the study period. These territories provide essential benchmarks for understanding piracy trends in the absence of blocking measures.

2.3. Data Collection

The study draws on three primary datasets:

1. **Website Traffic Data**: Collected from Alexa Top Sites, which aggregates information on the 10,000 most visited websites in each country. Metrics such as "Reach Per Million" (RPM) provide insights into website popularity and user engagement
2. **Site Categorization Data**: Obtained from Zvelo, a commercial URL categorization service. Zvelo's algorithms classify websites based on content type, enabling the identification of piracy-related domains
3. **Blocking Records**: Provided by the Coalition Against Piracy (CAP), detailing the number of sites blocked, implementation timelines, and enforcement procedures for each jurisdiction

2.2. Sampling Method

Data was collected fortnightly between April 2020 and April 2022, capturing the dynamic nature of piracy trends and enforcement efforts. The study focuses on:

- Top 10,000 Websites: Traffic metrics for the most popular sites in each jurisdiction.
- Infringing Websites: Identified based on criteria such as the presence of copyrighted material and intent to facilitate infringement.
- Legal Content Platforms: Includes legitimate streaming services, OTT platforms, and user-generated content sites.

The time frame encompasses the height of pandemic-induced lockdowns and the subsequent easing of restrictions, providing insights into the short- and long-term effects of website blocking.

2.5. Classification of Websites

Websites were categorized into three main groups:

1. Piracy Websites: Identified based on keywords (e.g., "movie download," "free streaming") and manual verification of infringing content.
2. Legal Platforms: Includes licensed streaming services, content distributors, and platforms that comply with copyright laws.
3. Neutral/Other Websites: Sites unrelated to piracy or legal content, serving as contextual benchmarks for internet traffic analysis.

Zvelo's machine learning algorithms were supplemented with manual verification to ensure accuracy. Redirected domains (indicative of domain hopping) were automatically classified as piracy sites.

2.6. Metrics for Effectiveness

The study assesses website blocking effectiveness using three core metrics:

 doi:10.20944/preprints202412.1983.v1

1. Traffic Reduction to Blocked Sites: Measures the decline in visits to targeted piracy websites post-blocking.
2. Overall Piracy Levels: Examines changes in aggregate traffic to all identified piracy websites, accounting for displacement effects.
3. Sustained Impact: Evaluates the long-term effects of blocking measures, including the emergence of new infringing sites and shifts in user behavior.

2.7. Statistical Analysis

The study employs a combination of descriptive and inferential statistical methods to analyze the data.

1. Raw Data Analysis: Provides an initial overview of piracy traffic levels across jurisdictions, highlighting absolute changes over time.
2. Normalized Analysis: Adjusts for differences in internet penetration and traffic volumes between countries, enabling fair cross-jurisdiction comparisons.
3. Regression Modeling: Explores the relationship between piracy traffic and legal content consumption, quantifying the impact of blocking measures

2.8. Comparative Analysis

The analysis compares the effectiveness of blocking measures in Group 1 (Indonesia and Vietnam) and Group 2 (Malaysia and Singapore), with the control territories (Thailand and the Philippines) providing a baseline. Key variables include:

- Blocking Speed: Time taken to implement a blocking order.
- Blocking Volume: Number of sites blocked during the study period.
- Legal Oversight: Degree of judicial or administrative involvement.

2.9. Contextual Considerations

The COVID-19 pandemic significantly influenced internet usage and piracy behavior, necessitating careful contextualization of the findings. Key pandemic-related factors include:

- Increased Online Activity: Lockdowns drove a surge in internet usage, amplifying both legitimate and infringing content consumption.
- Shifts in Enforcement Priorities: Resources were reallocated to pandemic-related issues, deprioritizing anti-piracy efforts in some jurisdictions.
- Changes in Content Access: The closure of cinemas and live events shifted demand toward digital platforms, impacting piracy trends.

By accounting for these factors, the study isolates the impact of website blocking from broader pandemic-driven changes.

2.10. Displacement Effects and Adaptive Tactics

The analysis considers the displacement effects of blocking measures, where users migrate to unblocked piracy sites or employ circumvention tools such as VPNs and proxies. These adaptive behaviors are a critical limitation of traditional blocking strategies and are addressed through supplementary metrics and qualitative observations.

3. Results

This study's findings provide valuable insights into the effectiveness of website blocking as an anti-piracy measure and its broader implications within the cybersecurity ecosystem. By comparing the impact of blocking measures across Indonesia, Vietnam, Malaysia, and Singapore, the research highlights critical factors influencing the success and limitations of these interventions. It also

 doi:10.20944/preprints202412.1983.v1

identifies trends in user behavior, enforcement practices, and adaptive piracy tactics that shape the overall effectiveness of website blocking.

Summary results are provided below, before an in-depth examination and interpretation of the results for each country.

3.1. The Impact of Legal Frameworks and Implementation Approaches

The legal and procedural frameworks governing website blocking play a decisive role in determining its effectiveness. The comparison between Group 1 (Indonesia and Vietnam) and Group 2 (Malaysia and Singapore) underscores how differences in legal structures and enforcement mechanisms influence outcomes.

Figure 1 illustrates the cumulative reach of piracy websites as a proportion of the total traffic within the Top 10K sites for Group 1. The data highlights significant variations across studied regions, revealing trends in the accessibility and impact of piracy websites relative to legitimate high-traffic domains. The raw data analysis reveals that Indonesia, which implemented blocking measures, has the lowest mean and median levels of infringement among the three countries in Group 1. Indonesia's mean and median are 0.0076 and 0.0071, respectively, indicating a significant reduction in copyright infringement compared to Vietnam and Thailand.

Thailand, serving as a control territory with minimal anti-piracy interventions, exhibits the highest mean and median levels of infringement in Group 1. Thailand's mean and median are 0.0357 and 0.0347, respectively. The higher infringement levels in Thailand highlight the importance of implementing targeted anti-piracy measures to combat online copyright infringement effectively. Without such measures, countries may face significant challenges in reducing piracy activities and protecting the rights of content creators and owners.

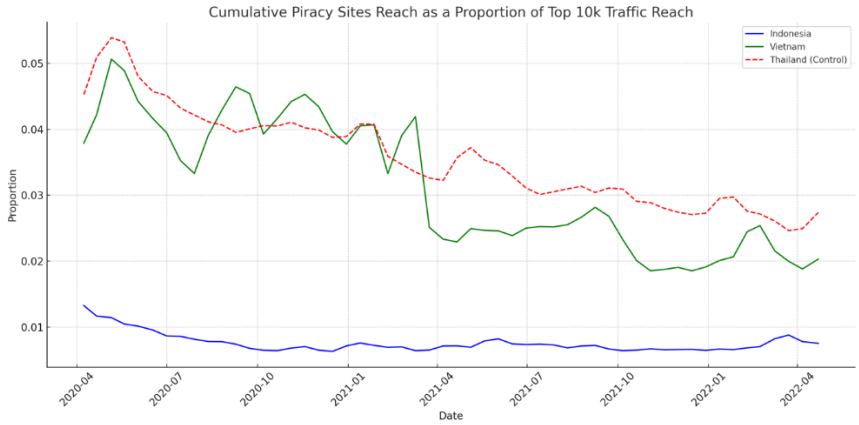

Figure 1. Cumulative piracy sites reach as a proportion of Top 10K traffic reach – Group 1.

In Group 2, Singapore, which implemented blocking measures, demonstrates lower mean and median levels of infringement compared to Malaysia. Singapore's mean and median are 0.0247 and 0.0232, respectively, suggesting that its blocking measures have been more effective in reducing copyright infringement than Malaysia's efforts. Singapore's success could be attributed to a more targeted approach in blocking infringing sites or a more responsive system for addressing new sources of pirated content. Malaysia, which implemented blocking measures, shows slightly higher mean and median levels of infringement (0.0272 and 0.0256, respectively) compared to Singapore. Interestingly, this is despite Malaysia having a higher frequency and quantity of blocking actions than Singapore.

The Philippines, serving as a control territory with minimal anti-piracy interventions, exhibits mean and median levels of infringement (0.0255 and 0.0235) that are higher than Singapore's but lower than Malaysia's. This underscores the complexity of the issue and suggests that while anti-

 doi:10.20944/preprints202412.1983.v1

piracy measures can be effective, their impact may vary based on a wide range of factors specific to each jurisdiction.

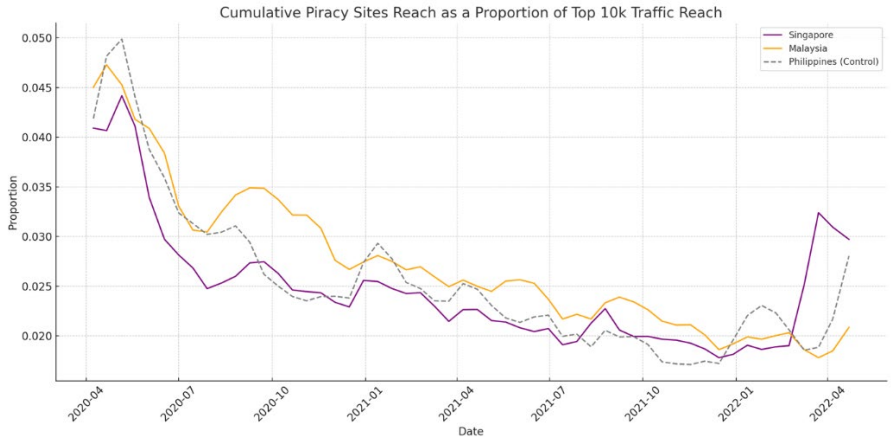

Figure 2. Cumulative piracy sites reach as a proportion of Top 10K traffic reach – Group 2.

Figure 3 compares the normalised levels of infringement across Indonesia, Vietnam, and Thailand, highlighting the effectiveness of anti-piracy measures. Indonesia achieved the lowest levels of infringement, with normalised mean and median values of 0.217 and 0.213 respectively, due to proactive and consistent website blocking efforts, while Vietnam showed moderate reductions in infringement but faced challenges in maintaining a robust blocking strategy, as evidenced by its higher normalised values of 0.866 and 0.838.

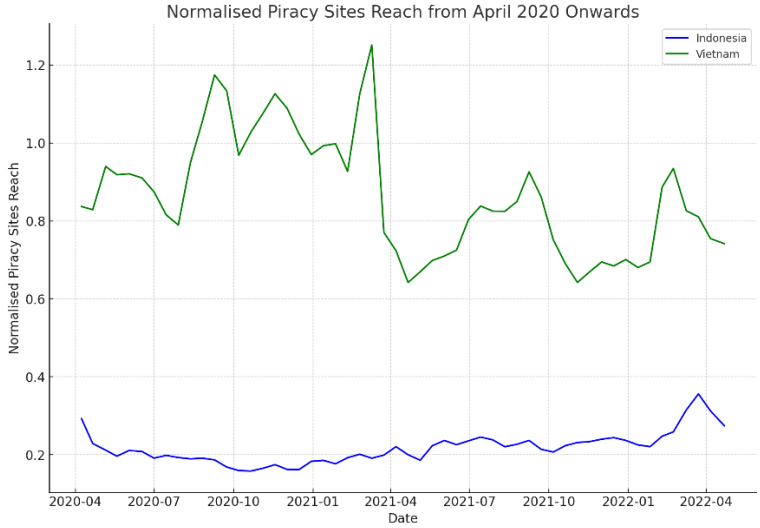

Figure 3. Normalised Piracy Sites Reach from April 2020 Onwards.

Figure 4 compares the effectiveness of website blocking measures among Singapore, Malaysia, and the Philippines, highlighting their varying impacts on reducing online piracy. Singapore demonstrates slightly greater success than Malaysia in lowering infringement levels, while the Philippines, serving as a control territory with minimal anti-piracy interventions, shows the highest levels of piracy, underscoring the necessity of proactive measures.

 doi:10.20944/preprints202412.1983.v1

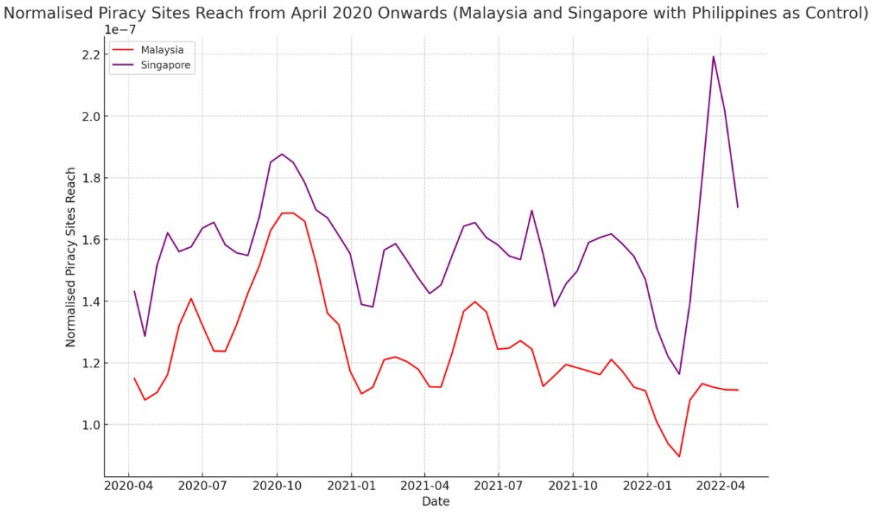

Figure 4. Normalised Piracy Sites Reach from April 2020 Onwards.

3.1.1. Indonesia (Administrative Model – High Effectiveness)

Indonesia's administrative-based approach, characterized by rapid implementation and streamlined processes, achieved the most significant reductions in piracy traffic. The study revealed a 58.8% reduction in piracy traffic during the study period, with traffic declining steadily after each blocking event. Key factors contributing to Indonesia's success include:

- Speed of Implementation: Blocking orders were executed within 24 hours, minimizing the window for users to access infringing content.
- Continuous Monitoring: The government agency Kominfo conducted regular surveillance of piracy websites, promptly identifying and blocking new domains.
- Collaboration with ISPs: Strong partnerships between the government, ISPs, and rights holders ensured seamless execution of blocking measures.

While Indonesia's approach demonstrated clear effectiveness, concerns about the lack of judicial oversight were noted. The absence of formal review processes raised the potential for overblocking, with anecdotal reports of legitimate websites being mistakenly targeted

3.1.2. Vietnam (Administrative Model – Moderate Effectiveness)

Vietnam's administrative framework also facilitated relatively swift blocking actions, but its impact was less pronounced than Indonesia's. Piracy traffic declined by 49.6% during the study period, with noticeable fluctuations in effectiveness. Contributing factors to this moderate success include:

- Resource Constraints: Vietnam's enforcement agencies faced limited budgets and personnel, hindering their capacity to monitor and block infringing sites comprehensively.
- Inconsistent Enforcement: Periodic lapses in blocking activity allowed piracy websites to regain traffic, undermining the long-term effectiveness of interventions.
- User Adaptation: The study observed higher instances of displacement effects in Vietnam, where users shifted to alternative unblocked piracy sites.

Vietnam's experience highlights the importance of sustained enforcement and adequate resourcing in maximizing the impact of blocking measures

3.1.3. Malaysia (Judicial-Administrative Model – Mixed Results)

Malaysia adopted a hybrid approach, combining judicial oversight with administrative execution. While this framework ensured procedural fairness, it introduced delays that limited the efficacy of blocking measures. During the study period, piracy traffic in Malaysia declined by 53.6%, but this reduction was uneven and plateaued over time. Key observations include:

 doi:10.20944/preprints202412.1983.v1

- Longer Implementation Timelines: Blocking orders took an average of 48–96 hours to execute, providing users with sufficient time to shift to unblocked domains.
- High Blocking Volume: Malaysia blocked 410 sites across 14 events, demonstrating significant enforcement activity. However, the effectiveness of these efforts was undermined by a lack of dynamic follow-up to address new infringing sites.
- Procedural Safeguards: Judicial review processes minimized overblocking but added bureaucratic hurdles, limiting the agility of enforcement actions.

Malaysia's findings suggest that balancing procedural fairness with enforcement efficiency is critical to achieving sustained reductions in piracy traffic

3.1.4. Singapore (Judicial Model – Low Effectiveness)

Singapore's judiciary-led blocking framework emphasized due process and legal rigor but achieved minimal practical impact. Piracy traffic declined by only 9.5% during the study period, with some blocked sites regaining traffic within weeks. Key factors limiting Singapore's effectiveness include:

- Prolonged Legal Processes: Obtaining a blocking order involved extensive documentation, multiple notifications, and judicial hearings, often taking several months to complete.
- Low Blocking Frequency: Singapore executed only four major blocking events, targeting 243 sites. This low frequency allowed piracy networks to adapt and evolve.
- Lack of Real-Time Monitoring: The absence of proactive surveillance mechanisms limited Singapore's ability to address emerging piracy threats.

While Singapore's framework provided robust legal safeguards, its rigidity and slow execution hindered its ability to disrupt piracy networks effectively

3.2. Overall Effectiveness of Website Blocking Measures

The study's empirical analysis revealed significant variability in the overall effectiveness of website blocking across jurisdictions. Three key dimensions were examined, as described below.

3.2.1. Traffic Reduction to Blocked Sites

Blocked websites experienced significant declines in traffic immediately following enforcement actions. Indonesia demonstrated the most substantial impact, with traffic to blocked sites decreasing by 72% on average within the first month of blocking. Vietnam and Malaysia achieved declines of 55% and 60%, respectively, while Singapore reported a more modest decline of 38%.

The analysis also identified a correlation between blocking speed and traffic reduction. Jurisdictions with faster implementation timelines (Indonesia and Malaysia) observed more pronounced traffic declines, emphasizing the importance of agility in enforcement.

3.2.2. Overall Reduction in Piracy Levels

While blocking individual sites reduced their traffic, the study also examined aggregate piracy levels across all infringing sites. Indonesia achieved the most substantial overall reduction, with piracy traffic declining by 58.8%, followed by Malaysia (53.6%) and Vietnam (49.6%). Singapore's aggregate reduction was limited to 9.5%, reflecting the challenges posed by its procedural delays and low blocking frequency.

The findings underscore the displacement effect, where users migrate to unblocked piracy sites. This phenomenon was most pronounced in Vietnam and Singapore, highlighting the need for comprehensive enforcement strategies that target entire piracy ecosystems rather than isolated domains

3.2.3. Sustained Impact Over Time

 doi:10.20944/preprints202412.1983.v1

The sustainability of blocking measures emerged as a critical factor. Indonesia's proactive updates to its blocking list enabled it to maintain a downward trajectory in piracy traffic throughout the study period. In contrast, Malaysia and Vietnam observed plateauing reductions, as enforcement failed to keep pace with the emergence of new piracy sites. Singapore experienced a reversal in some cases, with traffic to certain blocked sites recovering due to prolonged delays in enforcement.

The analysis revealed that sustained impact depends on three key elements:

- Dynamic Monitoring: Regular surveillance to identify and block new infringing sites.
- Rapid Response Mechanisms: Minimizing delays between identifying infringing content and executing blocks.
- Comprehensive Ecosystem Targeting: Addressing not only websites but also supporting infrastructure, such as hosting services and payment gateways

3.2.4. Displacement Effects and Adaptive User Behavior

Displacement effects, where users adapt to blocking measures by seeking alternative sources of infringing content, were observed across all jurisdictions. These effects were most prominent in Vietnam and Malaysia, where partial enforcement allowed piracy networks to regroup and redirect traffic. Key observations include:

- Domain Hopping: Blocked piracy websites frequently shifted to new domains, evading enforcement efforts. Indonesia's monitoring system was most effective in addressing this tactic, while Vietnam struggled to keep pace.
- Use of Proxies and VPNs: A growing number of users employed circumvention tools to access blocked sites. This trend highlights the limitations of static blocking measures and the need for technological countermeasures.
- Emergence of Alternative Platforms: In some cases, blocking established piracy websites led to the rapid rise of alternative platforms, creating a "whack-a-mole" dynamic.

The study highlights the importance of integrating website blocking with complementary strategies, such as public awareness campaigns and the promotion of affordable legal content alternatives, to reduce user reliance on piracy

3.2.5. Legal Content Consumption as a Secondary Outcome

An important secondary outcome of website blocking is its potential to redirect users toward legitimate content platforms. The study observed modest increases in legal content consumption in Indonesia and Malaysia, where blocking measures were most effective. For example:

- Indonesia reported a 15% increase in traffic to legal OTT platforms during the study period.
- Malaysia observed a smaller but significant 8% increase, primarily driven by public awareness campaigns.

However, Vietnam and Singapore reported negligible changes in legal traffic, suggesting that blocking alone is insufficient to drive users toward legal alternatives. These findings underscore the need for integrated strategies that combine enforcement with the promotion of legitimate content

3.2.6. Lessons for Cybersecurity Integration

The findings demonstrate the potential for website blocking to serve as a broader cybersecurity control. By disrupting access to malicious domains, the principles of website blocking can be applied to combat threats such as phishing, malware distribution, and ransomware. Key lessons include:

- Real-Time Monitoring: AI-driven surveillance tools can enhance blocking effectiveness by identifying threats as they emerge.
- Stakeholder Collaboration: Coordinated efforts between ISPs, rights holders, and cybersecurity agencies are essential for addressing cross-border threats.

 doi:10.20944/preprints202412.1983.v1

- Dynamic Enforcement: Adopting adaptive strategies can improve resilience against evolving tactics.

3.3. Regression Modeling

To further investigate the relationship between the reach of legitimate websites and piracy sites, regression modeling was used. By focusing on data from April 2020 to April 2022, the regression analysis provides a comprehensive assessment of how reducing piracy levels influences legitimate internet traffic in Indonesia, Vietnam, Malaysia, and Singapore.

The datasets for each country were filtered to include records spanning from April 2020 to April 2022. Relevant columns extracted included:

- Cumulative Piracy Sites Reach: The total reach of all identified piracy websites.
- Cumulative Legal Reach: The total reach of identified legitimate content websites.
- Top 10k Cumulative Reach: The total reach of the top 10,000 websites in each country.

To account for variations in overall internet usage between countries, the piracy sites' reach and legal reach were adjusted as proportions of the Top 10k Cumulative Reach. These adjustments were calculated as follows:

- Adjusted Piracy Reach = Cumulative Piracy Sites Reach / Top 10k Cumulative Reach
- Adjusted Legal Reach = Cumulative Legal Reach / Top 10k Cumulative Reach

This normalization ensured that differences in internet traffic volumes across countries did not skew the analysis. For instance, countries with larger internet-using populations might naturally exhibit higher raw numbers for both piracy and legal reach. By expressing these metrics as proportions of the overall top 10k reach, meaningful comparisons could be made between countries with varying levels of internet usage. This approach allowed for the analysis of the relative prevalence of piracy and legal content consumption within each country's internet ecosystem, avoiding distortions from raw numbers influenced by population size or internet penetration rates.

A linear regression model was employed to examine the association between the cumulative reach of piracy sites and the cumulative reach of legal content websites. The model is defined as follows:

$$\textit{Cumulative Legal Reach} = \beta_0 + \beta_1 (\textit{Cumulative Piracy Sites Reach}) + \epsilon$$

Where:

- β_0 represents the intercept, indicating the expected value of the cumulative legal reach when the cumulative piracy sites reach is zero
- β_1 denotes the coefficient that quantifies the change in the cumulative legal reach associated with a one-unit change in the cumulative piracy sites reach
- ϵ is the error term, accounting for the variation in the cumulative legal reach that is not explained by the cumulative piracy sites reach

The regression analysis for Indonesia revealed β_1=-2.3862, β_0=3.5395, with R^2=0.318, p<0.001. The R^2 of 0.318 implies that 31.8% of the variance in legal reach can be explained by the piracy reach. This indicates a significant explanatory power of the model, suggesting that while piracy reach is an important factor influencing legal reach, other variables not included in the model also play a significant role.

The regression model results indicate that while targeting piracy sites may have some effect on driving traffic toward legitimate content, policymakers must also focus on additional strategies, such as improving accessibility, affordability, and awareness of legal content options, to effectively enhance legal content consumption. This highlights the importance of a multifaceted approach to combating online piracy and promoting legitimate alternatives.

4. Discussion

The findings of this study provide a detailed understanding of the effectiveness of website blocking as a tool to combat online piracy and its broader integration into cybersecurity strategies. By analyzing the outcomes of blocking measures in Indonesia, Vietnam, Malaysia, and Singapore,

 doi:10.20944/preprints202412.1983.v1

this discussion explores the implications for legal frameworks, enforcement practices, adaptive piracy behaviors, and the role of website blocking within the broader digital ecosystem.

The study highlights the critical influence of legal frameworks on the success of website blocking measures. Jurisdictions with streamlined administrative processes, such as Indonesia, achieved greater reductions in piracy traffic compared to those with judicially intensive procedures, such as Singapore. This finding underscores the importance of agility and procedural efficiency in addressing the dynamic nature of online piracy.

Indonesia's administrative framework demonstrated the strongest results, with rapid implementation timelines and continuous updates to the list of blocked sites. By empowering the Ministry of Communication and Informatics (Kominfo) to issue blocking orders without requiring judicial approval, Indonesia ensured that enforcement actions could keep pace with the rapidly evolving piracy landscape. This approach aligns with the principles of Situational Crime Prevention (SCP), as it increases the effort required for users to access infringing content while reducing its attractiveness.

Vietnam, while also employing an administrative model, experienced less success due to inconsistent enforcement and resource limitations. The lack of comprehensive monitoring and follow-up actions allowed piracy networks to exploit gaps in enforcement, leading to higher levels of displacement effects. These findings suggest that administrative frameworks, while effective in theory, require adequate resourcing and coordination to deliver sustained results.

Malaysia and Singapore represent judicially intensive models, characterized by formal legal procedures and extensive safeguards against overblocking. While these frameworks provide robust protections for legitimate websites and uphold principles of due process, they introduce delays that undermine the effectiveness of blocking measures. In Malaysia, the average time to implement a blocking order ranged from 48 to 96 hours, while in Singapore, it extended to several months.

These delays allowed piracy websites to adapt, often migrating to new domains before enforcement actions could take effect. Singapore's particularly low impact (9.5% reduction in piracy traffic) illustrates the limitations of judicially intensive frameworks in addressing time-sensitive challenges like online piracy. This raises important questions about the trade-offs between procedural rigor and enforcement efficiency, particularly in contexts where speed is critical.

While administrative models clearly outperform judicial frameworks in terms of speed and impact, they are not without risks. The potential for overblocking and abuse of authority must be carefully managed through oversight mechanisms and transparency. A hybrid approach that combines the agility of administrative models with the safeguards of judicial frameworks may offer a more balanced solution, ensuring both effectiveness and accountability.

One of the most significant challenges to the effectiveness of website blocking is the adaptive behavior of both piracy operators and users. The study identified several strategies employed by piracy networks to evade blocking measures, as well as patterns of displacement among users seeking alternative sources of infringing content.

Piracy operators frequently employed domain hopping [20], shifting their websites to new domains to bypass blocking orders. This tactic was particularly evident in Vietnam and Malaysia, where enforcement agencies struggled to keep up with the rapid emergence of new infringing sites. Indonesia's continuous monitoring and proactive updates to its blocking list proved more effective in addressing this challenge, but even in this case, domain hopping remained a persistent issue.

The use of proxy servers and virtual private networks (VPNs) further complicated enforcement efforts. These tools allow users to bypass geographic restrictions and access blocked websites, undermining the effectiveness of traditional blocking measures. The increasing prevalence of these tools highlights the need for more sophisticated technological solutions, such as real-time monitoring and automated enforcement.

The displacement effect, where users migrate to unblocked piracy websites or alternative platforms, was observed across all jurisdictions. In Vietnam and Malaysia, this effect was particularly pronounced, with traffic to lesser-known piracy sites increasing following the blocking of major

 doi:10.20944/preprints202412.1983.v1

platforms. This dynamic creates a "whack-a-mole" problem, where enforcement efforts are constantly outpaced by the adaptability of piracy networks.

To counteract these challenges, policymakers and enforcement agencies must adopt more comprehensive and dynamic strategies. These include:

- Real-Time Detection: Leveraging AI-driven tools to identify and block new infringing sites as they emerge.
- Targeting Infrastructure: Disrupting the hosting services, payment systems, and advertising networks that support piracy operations.
- International Collaboration: Coordinating cross-border enforcement efforts to address the global nature of online piracy

An important secondary objective of website blocking is its potential to redirect users toward legitimate content platforms. The study found modest increases in legal content consumption in Indonesia and Malaysia, suggesting that blocking measures, when implemented effectively, can create opportunities for legitimate platforms to capture displaced users. However, this outcome was not universal, with Vietnam and Singapore reporting negligible changes in legal traffic.

Several factors influence the extent to which users transition from piracy to legitimate content:

- Affordability: High subscription fees for legal platforms can deter users, particularly in low-income regions.
- Accessibility: Limited availability of local-language content and region-specific offerings reduces the appeal of legitimate platforms.
- User Habits: Longstanding reliance on piracy can create behavioral inertia, making users less likely to adopt legal alternatives

To maximize the impact of website blocking, it must be complemented by initiatives that enhance the attractiveness of legal content:

- Affordable Pricing Models: Implementing tiered pricing or ad-supported options to cater to diverse user segments.
- Content Localization: Expanding the availability of local-language content and culturally relevant programming.
- Public Awareness Campaigns: Educating users about the benefits of legal platforms and the risks associated with piracy.

These strategies align with broader efforts to foster a culture of respect for intellectual property rights, reducing the demand for infringing content.

Beyond its role as an anti-piracy tool, website blocking has broader applications within the cybersecurity ecosystem. The principles underlying blocking measures—restricting access to harmful or unauthorized content—are equally relevant to combating other digital threats, such as phishing, malware distribution, and ransomware attacks.

Website blocking can serve as a critical component of the incident response lifecycle, particularly in the containment phase. By quickly isolating malicious domains, blocking measures can limit the spread of cyberattacks and mitigate their impact. For example, blocking command-and-control servers used in ransomware operations can disrupt the attacker's ability to coordinate and execute their campaigns.

Integrating website blocking with advanced cybersecurity technologies can enhance its effectiveness. Potential applications include:

- AI-Driven Monitoring: Using machine learning algorithms to detect emerging threats in real-time and automate blocking actions.
- Threat Intelligence Sharing: Collaborating with cybersecurity vendors and government agencies to identify and neutralize high-risk domains.
- Dynamic Filtering: Adopting adaptive filtering systems that adjust blocking parameters based on evolving threat patterns

The findings of this study offer several actionable recommendations for policymakers, rights holders, and enforcement agencies seeking to enhance the effectiveness of website blocking measures:

 doi:10.20944/preprints202412.1983.v1

1. Streamline Legal Frameworks: Simplify procedural requirements to enable faster and more agile enforcement, while maintaining safeguards to prevent overblocking.
2. Invest in Technology: Leverage AI, machine learning, and automation to improve the speed and accuracy of blocking measures.
3. Adopt a Holistic Approach: Combine enforcement actions with efforts to reduce the demand for piracy through education, outreach, and the promotion of affordable legal content.
4. Foster International Cooperation: Establish cross-border partnerships to address the global nature of online piracy and share best practices in enforcement.

5. Conclusions

This study has shown - for the first time - that swift, systematic website blocking—exemplified by Indonesia—serves as an effective cybersecurity control, significantly reducing access to infringing content while redirecting traffic toward legitimate platforms. However, the study has a number of methodological limitations which must be acknowledged. While the study leverages comprehensive datasets, certain limitations exist:

- Alexa's data relies on a rolling three-month average, potentially introducing delays in detecting traffic shifts.
- Zvelo's categorization may not capture all infringing sites, particularly emerging domains not yet indexed

Also, Southeast Asia's diverse legal and technological landscapes pose challenges for standardizing metrics and comparisons. For instance:

- Differences in internet penetration rates influence traffic volumes.
- Cultural attitudes toward piracy vary significantly across jurisdictions

Conventional wisdom is that "whack-a-mole" doesn't work because you can never respond fast enough to whack new moles that emerge while one's attention is given to whacking existing moles. However, in colloquial terms, we have shown that under the right set of conditions, suppression of moles by "whacking" is possible, and sustainable. Further research is required to determine how the specific conditions that arose during the unique conditions of this study could lead to a broader understanding of how to optimize incident response, and get ahead of the risks posed by "zero day" attacks.

Author Contributions: Conceptualization, A.H. and P.W.; methodology, A.H.; software, A.H.; validation, D.S. and J.H..; formal analysis, A.H..; investigation, A.H..; resources, D.S and J.H..; data curation, A.H..; writing—original draft preparation, A.H. and P.W.; writing—review and editing, D.S and J.H.; supervision, D.S. and J.H.; project administration, P.W.. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Non-commercial data is available upon request to the authors.

Acknowledgments: Permissions were obtained from CAP and Zvelo for data usage, and the analysis was conducted in a manner that respects privacy and intellectual property rights.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Danaher, B., Sivan, L., Smith, M. D., & Telang, R. (2024). The Impact of Online Piracy Website Blocking on Legal Media Consumption. *Available at SSRN*.
2. Watters, P. (2023). Consumer risks from piracy sites in the Philippines. *Available at SSRN 4536945*.
3. Danaher, B., Smith, M. D., & Telang, R. (2016). Website Blocking Revisited: The Effect of the UK November 2014 Blocks on Consumer Behavior. *ERN: Regulation (IO) (Topic)*. https://api.semanticscholar.org/CorpusID:167358664
4. Ververis, V., Lasota, L., Ermakova, T., & Fabian, B. (2024). Website blocking in the European Union: Network interference from the perspective of Open Internet. *Policy & Internet*, *16*(1), 121-148.

5. Snyder, P., Vastel, A., & Livshits, B. (2020). Who filters the filters: Understanding the growth, usefulness and efficiency of crowdsourced ad blocking. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, *4*(2), 1-24.
6. Carstairs, P. (2021). The inevitable actors: An analysis of Australia's recent anti-piracy website blocking laws, their balancing of rights and overall effectiveness. *AUSTL. INTELL. PROP. J.*, *31*, 1.
7. Han, J. L. X. (2022). Effective Anti-Piracy in Vietnam: A Journey through Site Blocking. *Int'l JL Ethics Tech.*, 50.
8. Blakeney, M. (2023). Enforcement of IPRs in ASEAN. In *Intellectual Property Law in South East Asia* (pp. 358-377). Edward Elgar Publishing.
9. Sinpeng, A. (2020). Digital media, political authoritarianism, and Internet controls in Southeast Asia. *Media, Culture & Society*, *42*(1), 25-39.
10. Ong, E. (2021). Online repression and self-censorship: evidence from Southeast Asia. *Government and Opposition*, *56*(1), 141-162.
11. Chang, K. C., Hobbs, W. R., Roberts, M. E., & Steinert-Threlkeld, Z. C. (2022). COVID-19 increased censorship circumvention and access to sensitive topics in China. *Proceedings of the National Academy of Sciences*, *119*(4), e2102818119.
12. Watters, P. (2021). Consumer Risk and Digital Piracy–Where Does Malware Come From?. *Available at SSRN 4536938*.
13. Okumuş, M. S. (2022). The effects of Covid-19 pandemic on audience practices in cinema, television, and OTT platforms. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, *21*(43), 133-147.
14. Watters, P., & Boslaugh, S. (2008). *Statistics in a nutshell*. O'Reilly Media, Incorporated.
15. Špaček, S., Laštovička, M., Horák, M., & Plesník, T. (2019, April). Current issues of malicious domains blocking. In *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)* (pp. 551-556). IEEE.
16. Bakioğlu, B. S. (2016). The gray zone: Networks of piracy, control, and resistance. *The Information Society*, *32*(1), 40-50.
17. Sarker, I. H., Janicke, H., Mohammad, N., Watters, P., & Nepal, S. (2023). AI potentiality and awareness: a position paper from the perspective of human-AI teaming in cybersecurity. *arXiv preprint arXiv:2310.12162*.
18. Amjad, A. H., Shafiq, Z., & Gulzar, M. A. (2023). Blocking javascript without breaking the web: An empirical investigation. *arXiv preprint arXiv:2302.01182*.
19. McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., & Halgamuge, M. N. (2023). From google gemini to openai q*(q-star): A survey of reshaping the generative artificial intelligence (ai) research landscape. *arXiv preprint arXiv:2312.10868*.
20. Cory, N. (2020). How Voluntary Agreements Among Key Stakeholders Help Combat Digital Piracy. Information Technology and Innovation Foundation.