Journal of Digital Law and Policy
Volume 3 Number 1, September 2023
e-ISSN 2808-3458 p-ISSN 2808-3652
https://ejournal.sidyanusa.org/index.php/jdlp

A Discussion of Malware Attacks Targeting Smart Homes and Connected Devices: Investigating Cybersecurity Risks in Everyday Living

I Gede Adnyana[1], Emmy Febriani Thalib[2], Mariano Alan Harum[3], Martha Apriliani Chionia Nagas[4], Martinus Wilfrid Jawa[5]

[1,2,3,4,5]*Institut Bisnis dan Teknologi Indonesia, Denpasar, Indonesia*

Email: [1]*adnyana.nakkuta@gmail.com*, [2]*emmy.febriani87@gmail.com*, [3]*harumalan3@gmail.com*, [4]*chyonianagas5@gmail.com*, [5]*martinjawa201@gmail.com*

Received on	*Revised on*	*Accepted on*
1 07 2023	*17 08 2023*	*15 09 2023*

Abstract

Computer technology has advanced with the digital age. Software for several platforms is crucial to streamlining human work with computers. This software is essential for many user tasks, including IoT ones. Through data exploitation and communication technologies, the Internet of entities (IoT) connects physical and virtual entities to the global web. This technology aims to make it easier for humans to interact with objects and let them communicate. In daily life, numerous specialized gadgets use the Internet of Things (IoT), especially Smart Homes. Smart Homes integrate networked communication networks with home devices for remote control, monitoring, and access. The name "Smart" in Smart Homes suggests intelligence, however IoT devices have limitations. Malware is purposely designed to disrupt or gain unauthorized access to computer systems without the system owner's knowledge or agreement. Malware threatens smart home security widely. Malware can also quickly regenerate and adapt as technology advances. It's often integrated into popular online apps. This study examines how malware assaults affect IoT and Smart Home devices. The study's conclusions include an analytical report on IoT and Smart Home malware mitigation in legal perspectives.

Keywords: *malware, IoT, Smart Home Devices*

INTRODUCTION

In the contemporary era characterized by rapid technology advancements, computers assume a crucial role in streamlining and facilitating various human jobs. Software functions on top of operating systems and plays a critical role in the execution of user tasks, persons in their professional endeavors. Nevertheless, it is important to acknowledge that not all software is developed with the purpose of aiding and optimizing human

activities. In fact, certain categories of software are specifically constructed with harmful intentions, resulting in detrimental consequences for individuals or groups.[1]

The incidence of cybercrime has exhibited an upward trend over the years, mostly propelled by the ongoing advancements in computer technology that significantly influence the daily lives of individuals. Despite the advantages derived from computer technology, it has unwittingly resulted in detrimental outcomes. Numerous persons using computer technology as a medium for engaging in unlawful acts that are in violation of legal statutes, driven by a variety of objectives that span from personal satisfaction to monetary benefits. Multiple techniques are utilized to enable cybercriminal activities using computer technology, which encompass the exploitation of network weaknesses through the deployment of software designed to illicitly acquire information, generally known as malware.[2]

Malware refers to a malicious software that is intentionally designed to cause harm or obtain unauthorized access to computer systems without the awareness or consent of the system owner. The presence of malware has the potential to cause significant disruption to computer systems and pose a serious risk of data theft. The development of malware is not a task undertaken by anyone indiscriminately; rather, it is the result of deliberate efforts by hackers possessing a profound comprehension of software, frequently driven by specific intentions.[3]

Malicious software, commonly referred to as malware, has the capability to penetrate computer systems via internet networks. This type of software manifests in diverse forms, including viruses, adware, Trojans, worms, botnets, and ransomware. It is worth mentioning that Trojan malware constitutes a substantial proportion of malware attacks in Indonesia, with adware being the subsequent prevalent type. Malware is commonly disseminated via unauthorized websites for downloads, deceptive emails designed to trick recipients, and other similar means. Moreover, malware has the capability to illicitly acquire stored data and function as an entry point for unauthorized individuals.

The modus operandi of cybercrime exhibits a wide range of strategies and is subject to constant evolution, as perpetrators employ ever intricate methods. Malware attacks encompass the utilization of worldwide internet networks to establish connections between physical and virtual entities, hence exploiting data and communication technologies.[4] The dissemination of these threats occurs through diverse channels, frequently involving the incorporation of malicious software within targeted applications or files.

The term "Internet of Things" (IoT) encompasses the interconnectedness of gadgets and the underlying technology that facilitates communication between devices and the cloud, as well as between devices themselves. The primary purpose of this system is to collect information and provide intelligent responses

---

[1] Faitouri A. Aboaoja et al., "Malware Detection Issues, Challenges, and Future Directions: A Survey," *Applied Sciences (Switzerland)* (MDPI, September 1, 2022), https://doi.org/10.3390/app12178482.

[2] Isaac Chin Eian et al., "Cyber Attacks in the Era of Covid-19 and Possible Solution Domains," *Preprints 2020*, no. September (2020).

[3] Rasa Bruzgiene and Konstantinas Jurgilas, "Securing Remote Access to Information Systems of Critical Infrastructure Using Two-Factor Authentication," *Electronics (Switzerland)* 10, no. 15 (2021), https://doi.org/10.3390/electronics10151819.

[4] Stanislaw Piasecki, Lachlan Urquhart, and Professor Derek McAuley, "Defence against the Dark Artefacts: Smart Home Cybercrimes and Cybersecurity Standards," *Computer Law and Security Review* 42 (September 1, 2021), https://doi.org/10.1016/j.clsr.2021.105542.

based on user interactions. In essence, the Internet of Things (IoT) encompasses all computational devices and associated technologies, regardless of their visibility. The foundation of the Internet of Things (IoT) is in the establishment of inter-machine connections or communication, facilitating independent interaction and operation based on obtained data, which can then be autonomously processed. The complexity of IoT systems can increase as the number of networked devices expands, hence facilitating the execution of more intricate activities. This technology enables efficient and uninterrupted connection with intelligent devices through the utilization of the internet.[5]

An emerging classification of intelligent gadgets pertains to Smart Homes, with a primary objective of augmenting household efficiency, safety, and internal network optimization. These devices have been specifically engineered to regulate and oversee the consumption of electricity, uphold optimal room temperature, administer garden maintenance, identify the presence of smoke, guarantee residential security, identify water leaks, and promptly notify homeowners.[6]

Nevertheless, although their sophisticated design, electronic gadgets that are connected to the internet or part of the Internet of Things (IoT) exhibit a significant susceptibility to assaults, specifically malware, owing to their convenient accessibility to the internet. As a result, the likelihood of successful restoration from devices infected with malware is frequently limited or unattainable. The restoration or updating of compromised Smart Home IoT equipment, including as refrigerators, home routers, televisions, and other electronically connected gadgets, can pose significant challenges.

Malicious software (malware) assaults targeting Internet of Things (IoT) devices often focus on exploiting vulnerabilities in internet-connected programs or botnets in order to spread malware, including ransomware. Malicious entities engage in the alteration of ostensibly harmless Smart Home gadgets, such as intelligent washing machines, with the intention of utilizing them for the purposes of botnet operations.

METHOD

A methodical methodology is needed to finish a legal academic work. Start by thoroughly proofreading and revising the text to correct grammar and formatting issues and ensure style guide citation consistency. Check for logical coherence and smooth section transitions in the article's structure and flow. Avoid jargon and write clearly to improve reader comprehension. Check all citations and references for accuracy and formatting, and cite important sources throughout the piece. Build solid arguments using precedents and current trends in a legal analysis. Legal analysis should inform policy recommendations. Rewrite the abstract to summarize the article's essential ideas, and in the conclusion, emphasize crucial findings. The article's content should address ethical issues, and formatting and style rules must be followed. Get peer, mentor, or legal advice to improve

[5] Haider Dhia Zubaydi, Pál Varga, and Sándor Molnár, "Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review," *Sensors* (MDPI, January 1, 2023), https://doi.org/10.3390/s23020788.

[6] Andrew P Mccoy and Armin Yeganeh, "An Overview of Emerging Construction Technologies," *NAIOP Research Foundation*, 2021, 1–45, https://www.researchgate.net/publication/350975155.

the article. Complete a thorough final check to ensure revisions and edits are applied consistently. The article fulfills academic standards and is ready for submission or publishing using this systematic technique.[7][8]

RESULT AND DISCUSSION

Legal Frameworks for Cybersecurity and IoT Devices

The present study examines the legal frameworks governing cybersecurity and Internet of Things (IoT) devices. This part commences the notion of Internet of Things (IoT) devices and its progressively pervasive integration into daily existence. The imperative for establishing legislative frameworks to govern cybersecurity within this realm is of utmost importance. Subsequently, undertake an examination of the prevailing legislative frameworks and regulatory measures pertaining to cybersecurity, with particular emphasis on Internet of Things (IoT) devices and Smart Homes. This essay will examine the manner in which various legal frameworks tackle significant concerns, including data breaches, privacy violations, and responsibility pertaining to cyberattacks on interconnected devices. This inquiry seeks to elucidate the efficacy of pertinent laws and regulations in ensuring the protection of Internet of Things (IoT) cybersecurity. To accomplish this, it is imperative to furnish instances of such regulations and evaluate their efficiency in preserving IoT cybersecurity.

Within the global context, there are numerous significant legislative and regulatory frameworks and efforts that pertain to the domain of cybersecurity and Internet of Things (IoT) devices:

1) The International Telecommunication Union (ITU), which operates as a specialized organization within the United Nations, has formulated a comprehensive set of rules and norms pertaining to the security and cybersecurity aspects of the Internet of Things (IoT). Their objective is to foster international collaboration in tackling cybersecurity issues related to Internet of Things (IoT) technologies.
2) The General Data Protection Regulation (GDPR) of the European Union (EU): The General Data Protection Regulation (GDPR) has substantial ramifications for Internet of Things (IoT) devices, with a primary emphasis on safeguarding data and ensuring privacy. The aforementioned regulation imposes stringent criteria pertaining to the gathering, manipulation, and safeguarding of personal information, specifically targeting Internet of Things (IoT) devices involved in the handling of this data.[9]
3) The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have collaborated to establish a range of standards pertaining to security and cybersecurity in the context of the Internet of Things (IoT). ISO/IEC 27001 and ISO/IEC 27002, among others, offer comprehensive recommendations pertaining to the implementation of information security management systems that are specifically relevant to the Internet of Things (IoT) domain.

---

[7] Ashleigh Watson, "Methods Braiding: A Technique for Arts-Based and Mixed-Methods Research," *Sociological Research Online* 25, no. 1 (2020), https://doi.org/10.1177/1360780419849437.

[8] Jianwei Hou, Leilei Qu, and Wenchang Shi, "A Survey on Internet of Things Security from Data Perspectives," *Computer Networks* 148 (January 15, 2019): 295–306, https://doi.org/10.1016/j.comnet.2018.11.026.

[9] EU GDPR, "GDPR Portal : Site Overview," 2018, https://www.eugdpr.org/.

4) The Organization for Economic Co-operation and Development (OECD) has released a set of principles pertaining to the Internet of Things (IoT) that prioritize the establishment of trustworthiness, with a particular focus on security and privacy concerns. These principles function as a structural foundation for the safe and secure implementation of Internet of Things (IoT) technology.
5) The EU Cybersecurity Act is a regulatory measure implemented by the European Union with the objective of bolstering the cybersecurity of digital products, namely encompassing Internet of Things (IoT) devices. This is achieved through the establishment of a comprehensive framework for cybersecurity certification. This policy promotes the adherence of manufacturers to cybersecurity standards.
6) The United Nations Commission on International Trade Law (UNCITRAL) has formulated the UNCITRAL Model Law on Electronic Transferable Records, which encompasses provisions pertaining to electronic transferable records, particularly those associated with the Internet of Things (IoT). These legislations facilitate the implementation of measures that enhance the security of electronic transactions and the use of digital signatures.

Global cybersecurity agreements and initiatives play a crucial role in fostering international collaboration to tackle the challenges posed by cybersecurity threats, which have significant implications for the security of the Internet of Things (IoT).[10] These agreements, such as the Budapest Convention on Cybercrime, and initiatives like the Paris Call for Trust and Security in Cyberspace, aim to facilitate collective efforts in addressing these threats and ensuring the integrity of IoT security. Industry standards and consortia play a crucial role in the development of guidelines and best practices for ensuring the security of the Internet of Things (IoT) across many industries. These organizations, such as the Industrial Internet Consortium (IIC) and the IoT Security Foundation, focus on creating internationally applicable recommendations for IoT security.[11]

The aforementioned instances of worldwide legal and regulatory frameworks and activities pertaining to cybersecurity in the Internet of Things (IoT) serve as illustrative examples. However, it is crucial to acknowledge that the dynamic nature of the IoT ecosystem and the emergence of novel difficulties necessitate ongoing developments in this domain. The establishment of collaboration among governments, industry players, and international organizations is necessary in order to guarantee a synchronized and comprehensive approach to the security of the Internet of Things (IoT) at a worldwide level.[12]

Based on the most recent information available as of September 2021, Indonesia has undertaken measures to tackle cybersecurity concerns and establish regulations pertaining to Internet of Things (IoT) devices.[13] It is

---

[10] Zharova Anna and Elin Vladimir, "State Regulation of the IoT in the Russian Federation: Fundamentals and Challenges," *International Journal of Electrical and Computer Engineering* 11, no. 5 (October 1, 2021): 4542–49, https://doi.org/10.11591/ijece.v11i5.pp4542-4549.

[11] Jenna Lindqvist, "New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?," *International Journal of Law and Information Technology* 26, no. 1 (March 1, 2018): 45–63, https://doi.org/10.1093/ijlit/eax024.

[12] Falguni Jindal, Rishabh Jamar, and Prathamesh Churi, "Future and Challenges of Internet of Things," International *Journal of Computer Science and Information Technology* 10, no. 2 (April 30, 2018): 13–25, https://doi.org/10.5121/ijcsit.2018.10202.

[13] Donovan Typhano Rachmadie and ' Supanto, "REGULASI PENYIMPANGAN ARTIFICIAL INTELLIGENCE PADA TINDAK PIDANA MALWARE BERDASARKAN UNDANG-UDANG REPUBLIK INDONESIA NOMOR

important to acknowledge that the regulatory environment is subject to change, and it is crucial to corroborate the most recent advancements by consulting official government sources and legal publications. The following are several fundamental elements pertaining to the regulation of Internet of Things (IoT) and cybersecurity in Indonesia:

1) The National Cybersecurity Agency, also known as Badan Siber dan Sandi Negara (BSSN), is an organization dedicated to the protection and defense of cybersecurity inside the nation. The Badan Siber dan Sandi Negara (BSSN) serves as the principal governmental entity entrusted with the coordination and supervision of cybersecurity initiatives inside the Republic of Indonesia. The entity in question assumes a pivotal role in the formulation of national policies and laws pertaining to the field of cybersecurity.
2) Indonesia has implemented data protection legislation, exemplified by the Personal Data Protection Bill, with the objective of governing the handling of personal data. The aforementioned restrictions have a significant influence on Internet of Things (IoT) devices that engage in the collection and processing of personal data.
3) The regulatory oversight of telecommunications and IoT connectivity is conducted by the Ministry of Communication and Informatics (Kominfo). Standards and regulations are established by regulatory bodies for providers of IoT connectivity.
4) Indonesia has recently implemented a Cybersecurity Law that encompasses rules pertaining to the safeguarding of critical information infrastructure (CII). Internet of Things (IoT) devices that are integrated into critical infrastructure may be subjected to distinct security prerequisites.
5) Industry-specific regulations exist in Indonesia for many industries, including banking and finance, healthcare, and transportation, which may be applicable to IoT devices working within these sectors. Frequently, these requirements encompass elements pertaining to cybersecurity and data protection.
6) The Indonesian government, in conjunction with industry stakeholders, has created standards for IoT security with the aim of fostering the secure development and deployment of IoT devices.
7) Indonesia actively engages in international endeavors and partnerships pertaining to cybersecurity and IoT security, thereby demonstrating its commitment to harmonizing with worldwide endeavors aimed at tackling these concerns.

It is important to note that the regulatory environment may have undergone changes since my previous update. To obtain the most up-to-date and accurate information regarding IoT and cybersecurity regulations in Indonesia, it is recommended to go to official government websites, seek guidance from legal professionals, or visit regulatory agencies inside the country.

Liability and Responsibility for Malware Attacks

The present subtopic aims to go into the intricate matter of accountability and responsibility pertaining to malware attacks targeting Internet of Things (IoT) devices. The prevention and mitigation of cyberattacks involve several stakeholders, namely device manufacturers, software developers, and end-users, each with distinct roles and responsibilities. Device manufacturers are responsible for producing hardware components

19 TAHUN 2016," *Recidive : Jurnal Hukum Pidana Dan Penanggulangan Kejahatan* 9, no. 2 (May 2, 2020): 128, https://doi.org/10.20961/recidive.v9i2.47400.

and devices that are resilient to cyber threats. Software developers play a crucial role in creating secure software applications and systems. End-users, on the other hand, are the individuals that utilize these devices and software, and their actions can significantly impact the overall security posture. By understanding the roles and responsibilities of these parties, we can better comprehend how they contribute to the prevention and resolution of cyberattacks. Perform an exhaustive examination of legal precedents and case law pertaining to the issue of responsibility in relation to malware attacks targeting Internet of Things (IoT) devices. This essay will examine the dynamic nature of legal standards and the inherent difficulties in assigning accountability. This inquiry seeks to explore the manner in which courts or regulatory bodies have ascertained legal responsibility in particular instances.

The legal and ethical implications surrounding malware attacks encompass the determination of accountability and responsibility, dictating the appropriate party to be held accountable in the event of such an attack.[14] Liability is to the legal obligation and liability an individual bears for their actions or failures to act.[15] Within the realm of malware assaults, the concept of responsibility pertains to the identification of individuals or entities that can be held accountable from a legal standpoint for the resultant damage or harm inflicted by the infection. Liability has the potential to encompass multiple entities within the cybersecurity ecosystem, encompassing:

1) Manufacturers of Internet of Things (IoT) devices can potentially face legal responsibility in the event that their devices has security vulnerabilities that have played a role in facilitating a malware attack.
2) Software developers can potentially be held responsible if their software applications or operating systems contain vulnerabilities that are exploited by malicious software.
3) End-users: In certain instances, end-users who neglect to implement adequate security measures, such as neglecting software updates or employing weak passwords, may bear partial responsibility if their actions or lack thereof have contributed to the occurrence of a malware attack.
4) Third parties may be subject to liability in the event of a malware attack, contingent upon the specific circumstances. These third parties encompass service providers, contractors, or suppliers whose activities or services have contributed to the occurrence of the assault.
5) Responsibility pertains to the moral or ethical duty to undertake suitable measures in order to avert harm or alleviate the repercussions of a virus intrusion. Responsibility encompasses a wider scope than mere legal culpability, encompassing the proactive actions undertaken by individuals or organisations to bolster cybersecurity, irrespective of their legal obligations. In the realm of cybersecurity, under the context of malicious software assaults,
6) Device manufacturers bear the obligation of designing and manufacturing devices that incorporate strong security measures, as well as ensuring the provision of security updates and patches to rectify any identified flaws.

---

[14] Minjung Park and Sangmi Chai, "Ai Model for Predicting Legal Judgments to Improve Accuracy and Explainability of Online Privacy Invasion Cases," *Applied Sciences (Switzerland)* 11, no. 23 (December 1, 2021), https://doi.org/10.3390/app112311080.

[15] Ayup Suran Ningsih, "The Doctrine of Product Liability and Negligence Cannot Be Applied to Malware-Embedded Software," *Journal of Indonesian Legal Studies* 4, no. 1 (May 1, 2019): 7–20, https://doi.org/10.15294/jils.v4i01.29157.

7) Software developers should place a high priority on incorporating security measures into their software design and development processes. It is crucial for developers to routinely update their software to effectively address any identified security vulnerabilities. Additionally, developers should provide comprehensive and unambiguous security recommendations to end-users, ensuring that they are equipped to utilize the program in a secure manner.
8) End-users are accountable for upholding the security of their devices and software by practices such as regularly updating them, employing robust passwords, and exercising caution when interacting with potentially dubious content.
9) Cybersecurity professionals are tasked with the job of recognizing and mitigating security vulnerabilities, promptly addressing occurrences, and continuously updating their knowledge of prevailing cybersecurity protocols.
10) Regulatory authorities and government agencies bear the obligation of formulating and implementing cybersecurity standards, regulations, and policies in order to safeguard the welfare of the general public.

In essence, liability pertains to the legal aspect of being held accountable, whereas responsibility involves the ethical and moral requirements associated with the prevention or resolution of malware attacks. Both characteristics are of utmost importance in shaping the responses of individuals, companies, and entities to cybersecurity issues and incidents. The allocation of culpability and duty may differ depending on the unique circumstances and the relevant laws and regulations in place.

Regulatory Challenges and Emerging Legal Trends

The legal viewpoint of IoT cybersecurity entails a shift in focus towards the regulatory difficulties and new trends in this field. This paper aims to elucidate the challenges inherent in the regulation of Internet of Things (IoT) devices, their extensive worldwide interconnection. This inquiry aims to examine the existing deficiencies and constraints within contemporary legislative frameworks pertaining to IoT cybersecurity rules, as well as the potential obstacles that may impede the efficient enforcement of such regulations. This discourse aims to examine the evolving legal patterns, encompassing proposed legislative measures and significant court decisions, which possess the potential to redefine the legal framework pertaining to cybersecurity in the context of the Internet of Things (IoT). This analysis examines the potential consequences of international factors, specifically focusing on the issues that arise across national borders and the efforts made to achieve harmonization in cybersecurity rules.[16]

The management of the ever-changing legal norms pertaining to liability and duty in the context of malware attacks poses numerous issues. This pertains to the changing nature of legal norms and the corresponding issues that arise. The concept of dynamic legal standards refers to the notion that legal norms and principles are subject to change and adaptation over time.

[16] Arka Ghosh, David John Edwards, and M. Reza Hosseini, "Patterns and Trends in Internet of Things (IoT) Research: Future Applications in the Construction Industry," *Engineering, Construction and Architectural Management* (Emerald Group Holdings Ltd., February 15, 2021), https://doi.org/10.1108/ECAM-04-2020-0271.

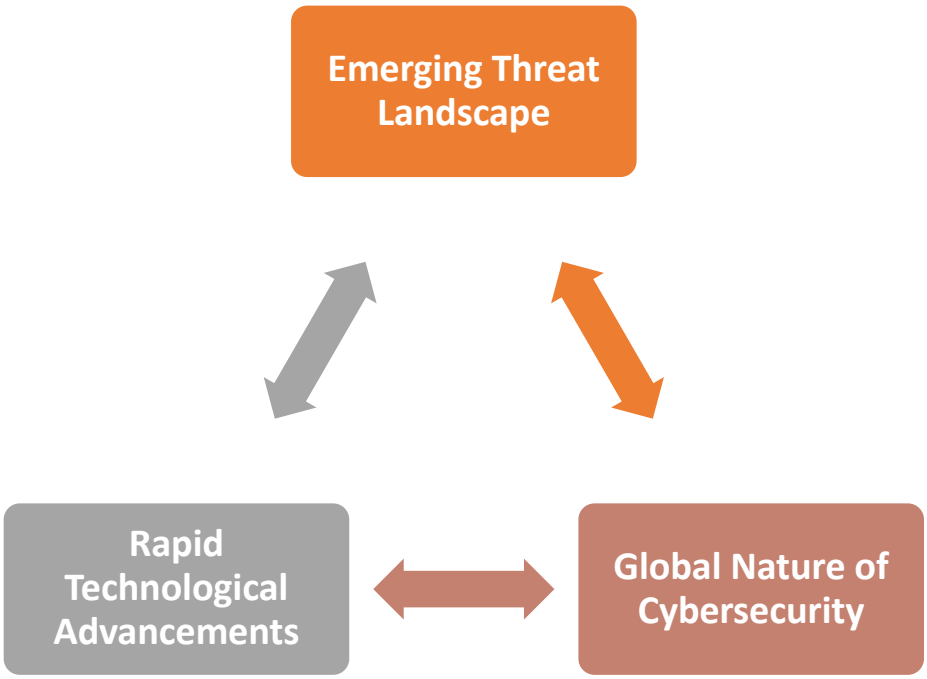

Figure 1. The Dynamic Legal Standart in Context of Regulatory Challenges
[Source: data processed by the author]

The ever-changing landscape of cybersecurity, encompassing the domain of malware attacks, is always developing. Regularly, there is a continuous emergence of new threats, attack strategies, and vulnerabilities. In order to effectively address these dynamic difficulties, it is imperative for legal standards to undergo necessary adaptations. The field of technology, encompassing many technologies such as Internet of Things (IoT) devices, is characterized by swift and significant advancements. It is imperative for legal norms to continually evolve in order to maintain their relevance and applicability in light of ongoing improvements in technology and security procedures.[17] The global nature of cybersecurity is seen in the fact that malware attacks transcend regional boundaries. These entities have the potential to originate from and exert influence over multiple countries. It is imperative for legal norms to adequately consider the worldwide scope of cybersecurity threats and effectively promote international collaboration.

The complexities associated with managing dynamic legal standards:[18]

1) An obstacle that arises is the discrepancy between technical advancements and the pace at which legislation is updated. The process of formulating, deliberating, and implementing new legislation or revising current legislation to effectively tackle evolving cybersecurity risks could necessitate a considerable amount of time.

[17] Bohdana Sereda and Jason Jaskolka, "An Evaluation of IoT Security Guidance Documents: A Shared Responsibility Perspective," in *Procedia Computer Science*, vol. 201 (Elsevier B.V., 2022), 281–88, https://doi.org/10.1016/j.procs.2022.03.038.

[18] Evandro L.C. Macedo et al., "On the Security Aspects of Internet of Things: A Systematic Literature Review," *Journal of Communications and Networks* (Korean Institute of Communication Sciences, October 1, 2019), https://doi.org/10.1109/JCN.2019.000048.

2) The Internet of Things (IoT) gadgets are integral components of a sophisticated and interdependent ecosystem. The attribution of culpability and assignment of blame in situations involving malware attacks that implicate many parties can provide significant challenges, particularly when the precise entity or device serving as the first point of entry for the attack remains uncertain.
3) The dynamic and ever-changing landscape of cybersecurity might give rise to legal ambiguity. The application of established laws to unprecedented circumstances can pose challenges for courts and regulatory entities, resulting in uncertainty when assigning legal responsibility.
4) Divergent International Standards: Discrepancies in legal standards and methods to cybersecurity may exist among various countries. The process of achieving international harmonization of these standards is a multifaceted endeavor, since it necessitates the reconciliation of divergent legal systems and cultural norms.
5) The issue of privacy concerns revolves around the perpetual struggle to strike a balance between the imperative for cybersecurity and the preservation of individual privacy rights. Certain cybersecurity methods have the potential to infringe upon individuals' privacy, hence giving rise to contentious discussions on the appropriate demarcation point.
6) Resource constraints can be a significant challenge for enterprises, particularly those of smaller scale, as they may face limitations in their ability to effectively adopt comprehensive cybersecurity measures. Ascertaining responsibility for these entities can pose difficulties when they themselves may be subjected to cyberattacks.

In order to establish robust legal norms, it is imperative for legal experts and legislators to engage in a process of continuous learning, specifically in the realm of cybersecurity advancements. Ongoing training and awareness are necessary in this context. And to effectively tackle these difficulties and respond to the ever-evolving legal landscape around cybersecurity and malware attacks, it is imperative to foster collaboration among governments, legal scholars, industry stakeholders, and cybersecurity practitioners. Effective legal solutions to growing cybersecurity concerns require the integration of multidisciplinary approaches, international cooperation, and a steadfast dedication to becoming knowledgeable about emerging risks and best practices.

CONCLUSION

Finally, the legal landscape for malware assaults on Internet of Things (IoT) devices is complex and changing. IoT cybersecurity is characterized by rapid technology breakthroughs and rising threats. Cybersecurity requires legal standards and frameworks to adjust with these advances. Device manufacturers, software developers, end-users, and regulatory authorities weigh in on malware culpability. Each party prevents and mitigates cyber threats differently. Cybersecurity is dynamic, therefore judges and regulators may struggle to apply current rules to new scenarios. This makes liability unclear. Cybersecurity risks cross boundaries, and IoT devices are part of a global ecosystem. Effectively addressing cross-border cyberattacks requires international cooperation and legislative harmonization. Smaller firms may struggle to deploy strong cybersecurity measures due to resource limits. Maintaining cybersecurity and privacy is difficult. To build and update effective legal standards, lawyers, policymakers, and cybersecurity specialists must continuously learn

about evolving dangers and best practices. Given these factors, addressing liability and responsibility for IoT malware attacks requires collaboration between governments, legal experts, industry players, and cybersecurity specialists. Enhancing IoT cybersecurity requires harmonizing worldwide standards, clarifying legal frameworks, and balancing security and privacy. The goal is to create a secure and resilient IoT ecosystem that protects all stakeholders from evolving cybersecurity threats.

REFERENCES

Aboaoja, Faitouri A., Anazida Zainal, Fuad A. Ghaleb, Bander Ali Saleh Al-rimy, Taiseer Abdalla Elfadil Eisa, and Asma Abbas Hassan Elnour. "Malware Detection Issues, Challenges, and Future Directions: A Survey." *Applied Sciences (Switzerland)*. MDPI, September 1, 2022. https://doi.org/10.3390/app12178482.

Anna, Zharova, and Elin Vladimir. "State Regulation of the IoT in the Russian Federation: Fundamentals and Challenges." *International Journal of Electrical and Computer Engineering* 11, no. 5 (October 1, 2021): 4542–49. https://doi.org/10.11591/ijece.v11i5.pp4542-4549.

Bruzgiene, Rasa, and Konstantinas Jurgilas. "Securing Remote Access to Information Systems of Critical Infrastructure Using Two-Factor Authentication." *Electronics (Switzerland)* 10, no. 15 (2021). https://doi.org/10.3390/electronics10151819.

Eian, Isaac Chin, Lim Ka Yong, Majesty Yeap Xiao Li, Yeo Hui Qi, and Zahra Fatima. "Cyber Attacks in the Era of Covid-19 and Possible Solution Domains." *Preprints 2020*, no. September (2020).

GDPR, EU. "GDPR Portal : Site Overview," 2018. https://www.eugdpr.org/.

Ghosh, Arka, David John Edwards, and M. Reza Hosseini. "Patterns and Trends in Internet of Things (IoT) Research: Future Applications in the Construction Industry." *Engineering, Construction and Architectural Management*. Emerald Group Holdings Ltd., February 15, 2021. https://doi.org/10.1108/ECAM-04-2020-0271.

Hou, Jianwei, Leilei Qu, and Wenchang Shi. "A Survey on Internet of Things Security from Data Perspectives." *Computer Networks* 148 (January 15, 2019): 295–306. https://doi.org/10.1016/j.comnet.2018.11.026.

Jindal, Falguni, Rishabh Jamar, and Prathamesh Churi. "Future and Challenges of Internet of Things." *International Journal of Computer Science and Information Technology* 10, no. 2 (April 30, 2018): 13–25. https://doi.org/10.5121/ijcsit.2018.10202.

Lindqvist, Jenna. "New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?" *International Journal of Law and Information Technology* 26, no. 1 (March 1, 2018): 45–63. https://doi.org/10.1093/ijlit/eax024.

Macedo, Evandro L.C., Egberto A.R. De Oliveira, Fabio H. Silva, Rui R. Mello, Felipe M.G. Franca, Flavia C. Delicato, Jose F. De Rezende, and Luis F.M. De Moraes. "On the Security Aspects of Internet of Things: A Systematic Literature Review." *Journal of Communications and Networks*. Korean Institute of Communication Sciences, October 1, 2019. https://doi.org/10.1109/JCN.2019.000048.

Mccoy, Andrew P, and Armin Yeganeh. "An Overview of Emerging Construction Technologies." *NAIOP Research Foundation*, 2021, 1–45. https://www.researchgate.net/publication/350975155.

Ningsih, Ayup Suran. "The Doctrine of Product Liability and Negligence Cannot Be Applied to Malware-Embedded Software." *Journal of Indonesian Legal Studies* 4, no. 1 (May 1, 2019): 7–20. https://doi.org/10.15294/jils.v4i01.29157.

Park, Minjung, and Sangmi Chai. "Ai Model for Predicting Legal Judgments to Improve Accuracy and Explainability of Online Privacy Invasion Cases." *Applied Sciences (Switzerland)* 11, no. 23

(December 1, 2021). https://doi.org/10.3390/app112311080.

Piasecki, Stanislaw, Lachlan Urquhart, and Professor Derek McAuley. "Defence against the Dark Artefacts: Smart Home Cybercrimes and Cybersecurity Standards." *Computer Law and Security Review* 42 (September 1, 2021). https://doi.org/10.1016/j.clsr.2021.105542.

Rachmadie, Donovan Typhano, and ' Supanto. "REGULASI PENYIMPANGAN ARTIFICIAL INTELLIGENCE PADA TINDAK PIDANA MALWARE BERDASARKAN UNDANG-UDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016." *Recidive : Jurnal Hukum Pidana Dan Penanggulangan Kejahatan* 9, no. 2 (May 2, 2020): 128. https://doi.org/10.20961/recidive.v9i2.47400.

Sereda, Bohdana, and Jason Jaskolka. "An Evaluation of IoT Security Guidance Documents: A Shared Responsibility Perspective." In *Procedia Computer Science*, 201:281–88. Elsevier B.V., 2022. https://doi.org/10.1016/j.procs.2022.03.038.

Watson, Ashleigh. "Methods Braiding: A Technique for Arts-Based and Mixed-Methods Research." *Sociological Research Online* 25, no. 1 (2020). https://doi.org/10.1177/1360780419849437.

Zubaydi, Haider Dhia, Pál Varga, and Sándor Molnár. "Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review." *Sensors*. MDPI, January 1, 2023. https://doi.org/10.3390/s23020788.