The Rising Threat on the Internet

Kunal Patel

Old Dominion University

Interdisciplinary Research Process and Theory 300W

Dr. Patricia Oliver

December 1, 2024

Abstract

This paper elaborates on the growing threats of cyber-attacks on the internet, from data breaches, ransomware, and social engineering to an attack on critical infrastructure. Based on the interdisciplinary framework of cybersecurity law, sociology, and psychology, the paper will discuss the technical and human factors contributing to online risks. Findings indicated a need for a concerted approach against these cyber threats. An interdisciplinary approach to technical solutions merging with human-centered strategies and legal framework enhances the mitigation of cyber risks toward a more secure society in cyberspace.

Introduction

The digital transformation is fast-changing modern society, becoming an indispensable part of daily lives: communication, commerce, and government functions. However, the increasing interconnectivity of systems has made the internet a prime hunting ground for cybercriminals. Cyber-attacks-including but not limited to data breaches, ransomware, and phishing-are becoming more routine and sophisticated, posing a growing threat to individuals, organizations, and governments. These threats are not just technical challenges but will be treated sociologically and psychologically since they rely on some level of human behavior or social dynamics. Therefore, responding to cyber threats requires more than a technical fix-it requires an interdisciplinary approach. This paper proposes an integrated framework to tackle cyber risks and enrich the geography of resistance by matching cybersecurity perspectives with those of sociology, law, and psychology.

Cybersecurity in Addressing Internet Threats

Cyber threats-targeting the security of digital systems range from legacy malware and ransomware to more recently emerging phishing schemes and advanced persistent threats (APTs)-have been reliant upon a range of computer networking vulnerabilities and human behavioral weaknesses. Classical measures still hold their mark, yet none are suitable for a rapidly changing world of criminal behavior. This deficiency has fueled a growing adoption of artificial intelligence (AI) and machine learning (ML) in cybersecurity. Easing through billions of bytes of information in an instant allows swifter recognition of also crippling anomalies that indicate looming attacks (Gupta et al., 2023). The hack by a machine-learning algorithm could make an unprecedented alteration in attack vs. defense perfection. The mix of AI and human analysis hurdles the extent at which criminals utilize machine learning in constantly fine-tuning ways of evading cybersecurity. This does not mean that humans will completely outshine machines, though: it will only solidify the presence of the humans aiding the smooth running of AI-adopted cybersecurity against cybercrime.

Psychological Impact of Internet Threats

The psychological dynamics of cyber threats are critical to understanding how attacks are carried out and their long-term effects on victims. Cybercriminals often exploit psychological vulnerabilities through social engineering, manipulating individuals into divulging sensitive information or clicking on malicious links. For instance, phishing scams prey on emotional triggers, such as fear or urgency, to deceive users into revealing personal details (Information Resources Management Association, 2010). These attacks, while being very hurtful at the moment, also leave psychological scars. Victims of cybercrime often report anxiety, reduced trust in digital systems, and a general fear of future victimization. On one aspect, research has

identified that some cybercrimes, like identity theft, have several post-victimization effects on the targets that could extend over months and even years. Because of this fact, cybersecurity should include technical strategies to protect these resources and mental and emotional impacts on an individual (Jones, 2022). In addition, digital platforms must mitigate the above psychological effects and build public trust and confidence through effective support systems and awareness campaigns.

Sociological Factors Contributing to Internet Vulnerabilities

Hence, the sociology of cybersecurity helps us understand how social dynamics create vulnerabilities on the internet. First is the digital divide, referring to the gap in access to technology and skills within various socioeconomic groups and geographic divisions. Communities with limited resources in technology or cybersecurity skills will be more vulnerable to such attacks. For example, less exposed to digital technologies, old citizens became targets of phishing scams. In underprivileged areas, even the minimal resources to deploy minimum cybersecurity may be absent, turning them into easy victims of cybercrime. Adding to that is the lack of understanding of the consequences of overspreading information among the general public; very few are conversant with the possible dangerous scenarios one opens up to while using social networks. For this, much-needed sociological vulnerabilities may be countered with public awareness campaigns and education. Government initiatives and community-based education efforts to improve digital literacy can help bridge the gap and reduce the risks associated with cybersecurity (Weaver et al., 2024). Enhancing public understanding of privacy and security practices is vital to fostering a more resilient and informed online society.

Legal and Regulatory Responses to Internet Threats

Legal frameworks create a vital foundation for managing cyber threats by ensuring norms for data privacy and setting accountability in case of breach. Laws such as the General Data Protection Regulation (GDPR) of the European Union provide some precedents regarding the protection of personal information and accountability for data security (Elendu et al., 2024). However, the global nature of the internet poses some administrative challenges in uniform enforcement of these laws. Cybercriminals often operate in multiple jurisdictions. It becomes difficult for one country to exercise control and enforce legal provisions. Hence, international cooperation and harmonization of cybersecurity laws are becoming recognized as necessary. Some of these treaties and agreements, such as the Budapest Convention, generally recognize looking for cooperation and the harmonization of laws against acts of cybercrime (Quigley, 2008). While these are commendable efforts, there is still a tough road ahead as general regulation is complex due to the plurality of legal systems and national interests. It is high time, at this juncture, that countries continue to develop a joint effort to develop a flexible legal framework to ensure that cyber threats do not constantly develop in the same direction.

Addressing the Threat through an Interdisciplinary Approach

It calls for an interdisciplinary approach where the cybersecurity expert integrates technical solutions with insights from psychology, sociology, and law in dealing with the growing threats over the internet. This will be in collaboration with psychologists to develop better training programs designed to teach how to identify social engineering attacks and ways of avoiding them. Sociologists can contribute to that by pointing out the social and economic factors, like the digital divide, that make people more vulnerable while asking for public education campaigns that increase digital literacy. It requires legal experts to create policies protecting data privacy, ensuring accountability, and creating international cooperation. When working in cooperation, these expert professionals in diverse fields can make a comprehensive, workable cybersecurity approach to cyber threats' technological and human components. In so doing, one enhances the security position and public confidence in digital systems, a precondition for a safer, more secure digital society.

Conclusion

The threats from cyber criminals through the internet are an evolving and complex challenge involving several approaches. While technological solutions, including AI-driven cybersecurity systems, are needed, they are insufficient. A multidimensional strategy should cover not only the psychological, sociological, and legal aspects of cybersecurity but also, by integrating knowledge from these different fields, more robust defenses against cybercrime can be created that also consider the human and social factors involved rather than just technical vulnerabilities. Where the digital landscape is constantly evolving, mitigation efforts through interdisciplinary collaboration will answer the risks associated with cyber threats to ensure a safe and resilient internet for all.

Works Cited

Weaver, G., Edwards, J., Edwards, J., & Weaver, G. (2024). International Cybersecurity Laws and Regulations. In The Cybersecurity Guide to Governance, Risk, and Compliance (pp. 299–314). John Wiley & Sons, Incorporated. https://doi.org/10.1002/9781394250226.ch17

Information Resources Management Association. (2010). International journal of cyber behavior, psychology, and learning. IGI Pub.

Elendu, C., Omeludike, E. K., Oloyede, P. O., Obidigbo, B. T., & Omeludike, J. C. (2024). Legal implications for clinicians in cybersecurity incidents: A review. Medicine (Baltimore), 103(39), e39887. https://doi.org/10.1097/MD.0000000000039887

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. IEEE Access, 11, 1–1. https://doi.org/10.1109/ACCESS.2023.3300381

Quigley, M. (2008). Encyclopedia of information ethics and security. Information Science Reference