Media, Culture and Public Relations Vol.17, 1

INFO - 200 UDK 004.056:34:17

https://doi.org/10.63191/mcpr.17.1.2 ORIGINALNI ZNANSTVENI RAD / ORIGINAL SCIENTIFIC PAPER

LEGAL AND ETHICAL RESPONSIBILITY IN UNWITTING DDOS/DRDOS PARTICIPATION

Krunoslav Antoliš
Professor of higher education permanent
Chief Police Adviser
member of the steering committee of the University of Applied Sciences in Criminal Investigation and Public Security, Ministry of Internal Affairs, Republic of Croatia

ABSTRACT: The digital space is becoming increasingly complex, and cyberattacks such as DDoS and DRDoS pose serious threats to critical infrastructure, corporations, and individuals (Zengupta et al., 2021). A key issue in this context is the question of responsibility when a computer owner is unaware that their device has been compromised and is being used in an attack. This paper analyzes the legal, technical, and ethical aspects of responsibility in the digital space through three research questions: (1) how legal frameworks treat the responsibility of owners in cases of ignorance, (2) which technical measures can prevent involuntary participation in attacks, and (3) whether there is an ethical obligation for society to educate users.

The methodological approach includes a qualitative analysis of literature, legal documents (EU NIS2 Directive, U.S. CFAA), case studies (Mirai botnet), and expert work on cybersecurity. The results show that most legal systems do not penalize users who are unaware of an infection unless they exhibit gross negligence (Schjolberg, 2017). However, the technical unpreparedness of users necessitates the redistribution of responsibility to software manufacturers, ISPs, and government agencies. Ethical analysis emphasizes the collective nature of cybersecurity and the need for systematic education (Livingstone et al., 2021).

KEYWORDS: Cybersecurity Responsibility, DDoS/DRDoS Attacks, Botnet Involvement, Legal and Ethical Frameworks, Shared Responsibility Model

INTRODUCTION

The rapid expansion of digital infrastructure has fundamentally reshaped how societies operate, enabling global communication, economic interdependence, and the seamless functioning of essential services. Yet this same interconnectedness has introduced new vulnerabilities. Cyberattacks—particularly Distributed Denial of Service (DDoS) and Distributed Reflection Denial of Service (DRDoS) attacks—have become increasingly sophisticated, frequent, and disruptive. They target not only private corporations but also hospitals, government agencies, financial institutions, and critical infrastructure, underscoring the fragility of the systems that underpin modern life (Zengupta et al., 2021). As digital ecosystems grow more complex, ensuring their resilience becomes a central concern for policymakers, security professionals, and society at large.

A major challenge within this landscape is the widespread use of botnets composed of compromised devices whose owners are unaware of their participation in malicious activity. The proliferation of Internet of Things (IoT) devices—often shipped with weak default credentials, limited update mechanisms, and minimal security controls—has dramatically expanded the pool of exploitable systems. Scholars such as Kolias et al. (2017) and Antonakakis et al. (2017) have shown how large scale botnets like Mirai leveraged these weaknesses to launch unprecedented attacks, demonstrating how everyday consumer devices can be weaponized at scale.

This raises complex legal and ethical questions. Traditional legal frameworks were not designed for a world in which individuals may unknowingly contribute to cybercrimes simply by owning insecure devices. Researchers have highlighted the ambiguity surrounding user responsibility, with some arguing that negligence in device maintenance may constitute a form of contributory fault (Brenner, 2010), while others emphasize the structural nature of the problem, pointing to manufacturers' obligations to implement secure by design principles (Woods & Simpson, 2017). Ethical debates further complicate the issue: to what extent can society expect non expert users to understand cybersecurity risks, and who bears responsibility for educating them?

Understanding these tensions is essential for building a more secure digital environment. As cyber threats continue to evolve, clarifying the boundaries of responsibility and strengthening preventive measures becomes not only a legal necessity but a societal imperative.

RESEARCH QUESTIONS

This paper examines the legal and ethical dimensions of this issue by addressing the following research questions:

- How do legal frameworks treat the responsibility of computer owners in cases of ignorance?
- What technical and organizational measures can reduce the risk of involuntary participation in cyberattacks?
- Is there an ethical obligation for society to educate users about cybersecurity?

METHODOLOGY

The research is based on a qualitative analysis of existing literature, including legal documents, case studies, and expert articles. The following methods were used:

- Legal analysis, focusing on EU regulations (e.g., the NIS Directive) and U.S. laws (such as the Computer Fraud and Abuse Act) to determine current approaches to user responsibility.
- Case studies, examining well known incidents where botnets were used without the owners' knowledge (e.g., the Mirai botnet case).
- Expert literature review, conducting a systematic analysis of scholarly works on cybersecurity, digital ethics, and user responsibility.

This research adheres to principles of methodological transparency. All legal documents, case studies, and scholarly sources used in the analysis are publicly accessible, and the criteria for their selection are explicitly described. The analytical procedures—including legal interpretation, comparative analysis, and literature synthesis—are fully documented to enable replication and critical asse-

ssment. No proprietary datasets or confidential information were used.

The author declares that there are no conflicts of interest influencing the research design, analysis, or conclusions presented in this paper.

OBJECTIVES OF THE STUDY

In addition to addressing the research questions, this work pursues several broader theoretical and analytical objectives that clarify its contribution to the field:

- To conceptualize the problem of involuntary participation in cyberattacks by examining how botnets exploit structural weaknesses in digital infrastructure and user practices.
- To analyze and compare existing legal frameworks in the EU and the U.S. in order to identify how different jurisdictions define, assign, or limit user responsibility in cases of unintentional involvement in cybercrime.
- To evaluate the ethical dimensions of user responsibility, particularly the extent to which non-expert users can reasonably be expected to understand and manage cybersecurity risks.
- To identify and systematize technical and organizational measures that can reduce the likelihood of device compromise, with a focus on security by design principles, regulatory mechanisms, and user oriented preventive strategies.
- To develop a clearer theoretical understanding of shared responsibility in cybersecurity, highlighting the interdependence between users, manufacturers, service providers, and regulatory bodies.
- To contribute to ongoing academic and policy debates by offering a structured analysis that connects legal, ethical, and technical perspectives into a coherent framework.

LEGAL ASPECTS OF RESPONSIBILITY IN DDOS/DRDOS ATTACKS

Liability for cyberattacks in most jurisdictions is based on intent and reasonable expectation (Schjolberg, 2017). Computer owners are generally not held liable if they were unaware of malware infections unless they demonstrated gross negligence, such as failing to install basic security updates.

The Concept of Liability in Cybercrime

The legal treatment of responsibility for cyberattacks, including Distributed Denial of Service (DDoS) and Distributed Reflective Denial of Service (DRDoS) attacks, is grounded in the principles of mens rea (intent) and due diligence (Schjolberg, 2017). Most legal systems hold that device owners cannot be prosecuted if they were unaware their systems had been compromised—unless gross negligence can be demonstrated (Wall, 2024). Gross negligence may be established through various forms of carelessness, such as failure to apply basic security updates (Kerr, 2018), continued use of software with known vulnerabilities, or ignoring antivirus warnings. In these circumstances, even if the user did not actively participate in the attack, their inaction may still be deemed a contributing factor to the cyber threat, thereby attracting legal scrutiny.

Legal Frameworks in the European Union

The European Union regulates cybersecurity primarily through the Network and Information Security Directive (NIS2) (EU Parliament, 2022), which mandates that users and organizations implement "reasonable protective measures" to enhance cyber resilience. These measures include regular software updates, the use of antivirus solutions, and education on basic cybersecurity practices. Failure to adopt such precautions may result in users being held partially liable for damages resulting from cyberattacks, although this liability is typically civil rather than criminal in nature. Notably, NIS2 places a greater burden of responsibility on key digital service providers—such as internet service providers (ISPs) and cloud service providers—than on individual users, reflecting the broader impact these entities have on the cybersecurity ecosystem.

U.S. Regulation: Computer Fraud and Abuse Act (CFAA)

In the United States, the primary legal framework for addressing cybercrime is the Computer Fraud and Abuse Act (CFAA) (Kerr, 2018). The CFAA makes a clear distinction between unwitting participation—such as when a user's device is infected by a botnet without their knowledge—and willful ignorance of security vulnerabilities. In cases of unknowing involvement, users are generally not held liable. However, when users demonstrate willful blindness to security flaws, such as knowingly using outdated, vulnerable software or refusing to install critical security patches, they may face civil or even criminal penalties. Case law, such as United States v. Nosal (2016), illustrates that prosecutions typically occur only when there is clear evidence of such willful negligence.

Comparative Analysis of Other Jurisdictions

Cybersecurity laws vary significantly across jurisdictions, reflecting differing approaches to user responsibility and liability. In the United Kingdom, the Computer Misuse Act 1990 requires proof of intent for establishing criminal liability, meaning users are generally not prosecuted unless it can be shown that they deliberately engaged in or facilitated cyber offenses. In contrast, Germany's Strafgesetzbuch (StGB) § 202c imposes penalties for failing to prevent the misuse of digital systems, but only if the user was aware of the potential risks and chose not to act (Gercke, 2012). Japan adopts a stricter stance: under its cybersecurity laws, users may be fined even if they were unaware their systems were infected, provided they neglected basic protective measures such as antivirus software or system updates. These variations underscore how national legal systems balance intent, awareness, and due diligence in assigning responsibility for cyber incidents.

Trends in International Law

There is growing international pressure to harmonize cyber liability standards through frameworks such as the Budapest Convention on Cybercrime (Council of Europe, 2001). This convention focuses on prosecuting key actors—such as botnet operators—rather than ordinary users, and emphasizes the responsibility of states to educate the public on basic cybersecurity practices. Despite these efforts, a universal consensus on the extent of user responsibility for cyberattacks they unknowingly facilitate remains elusive.

Legal approaches to Distributed Denial of Service (DDoS) and Distributed Reflective Denial of Service (DRDoS) attacks without the owner's knowledge generally hinge on proving either intent or gross negligence. While both the European Union and the United States have developed legal protections for users who are genuinely unaware of their systems being compromised, there is a noticeable trend toward assigning partial liability to those who neglect fundamental cybersecurity measures, such as installing updates or using antivirus software. As the global digital environment continues to evolve, future regulations are expected to strike a more defined balance between protecting innocent users and upholding a standard of societal responsibility in preventing cyber threats.

TECHNICAL RESPONSIBILITY AND DDOS/DRDOS ATTACK PREVENTION

Research indicates that many users lack the technical knowledge to detect infections. Consequently, responsibility often shifts to software manufacturers for vulnerabilities in operating systems, internet service providers (ISPs) capable of detecting botnet activity, and government agencies tasked with public education and oversight.

Limited Technical Preparedness of Users

Studies have shown that the majority of users are unable to recognize signs of malware infections or botnet activity on their devices. The Norton Cyber Security Insights Report (2022) further highlights this issue, revealing that 64% of users do not know how to check whether their computer has been compromised. This widespread lack of awareness underscores the need for a model of shared responsibility in cybersecurity. To effectively mitigate cyber risks, responsibility must be distributed among key stakeholders: software manufacturers, who must prioritize secure design and regular updates; internet service providers (ISPs), who can implement network-level protections and alert users to suspicious activity; and government or regulatory agencies, which play a crucial

role in setting standards, raising public awareness, and enforcing compliance.

Responsibility of Software Manufacturers

Operating system and application developers play a critical role in the prevention of Distributed Denial of Service (DDoS) attacks, as unpatched software vulnerabilities are a common gateway for botnet infections (Allodi et al., 2017). Delays in releasing or applying security updates significantly increase the risk of exploitation (Arzt et al., 2018). To mitigate these threats, industry leaders have adopted proactive security measures. For example, Microsoft's implementation of automatic Windows updates has significantly reduced the number of vulnerable devices (Microsoft Security Report, 2023), whereas Google's Project Zero initiative accelerates the patching process by publicly disclosing critical vulnerabilities to developers (Google, 2021). Despite these advances, some manufacturers continue to lag in addressing known threats, thereby perpetuating long-term cybersecurity risks and contributing to the broader vulnerability of the digital ecosystem (Zetter, 2014).

Role of ISPs in Detection and Prevention

Internet service providers (ISPs) are uniquely positioned to mitigate botnet activity and play a vital role in preventing DDoS attacks. By analyzing network traffic for anomalies, ISPs can detect early signs of malicious behavior (Dainotti et al., 2017), and by blocking suspicious IP addresses, they can prevent compromised devices from being recruited into the botnets. Several successful ISP-led initiatives highlight the effectiveness of such interventions. For example, the Cleaner DNS project in the Netherlands enables ISPs to automatically block communication with known botnet command-and-control servers, significantly reducing the spread of infections (van Rijswijk-Deij et al., 2016). Similarly, in the United States, the Federal Communications Commission (FCC) has introduced an Anti-Bot Code of Conduct, which encourages ISPs to monitor their users' networks and take action when signs of infection are detected. These efforts demonstrate how ISPs can serve as a crucial line of defense in the broader cybersecurity landscape.

Government Agencies and Regulatory Oversight

Governments play a central role in strengthening cybersecurity by fostering awareness, coordination, and innovation. A key responsibility is educating users on basic cyber hygiene to reduce the likelihood of unintentional participation in cyberattacks. Governments also act as intermediaries, facilitating collaboration between ISPs and software or hardware manufacturers to ensure timely responses to emerging threats, as emphasized in the EU's NIS2 Directive (EU, 2022). Additionally, public funding of cybersecurity research is crucial for developing advanced detection and prevention methods, such as those supported by the U.S. National Science Foundation. Several national initiatives reflect this proactive approach: Germany's BSI Bürger-CERT issues alerts to inform the public about new threats and vulnerabilities, whereas the U.S. The Cybersecurity and Infrastructure Security Agency (CISA) offers its "Shields Up" campaign to provide guidance on improving resilience against attacks (CISA, 2022). These efforts highlight the pivotal role of the government in building a secure and informed digital society.

Technical Solutions for Individuals and Organizations

Users and enterprises can reduce risks through:

Measure	Description	Efficacy (Study)
Regular updates	Installing OS/application patches	87% risk reduction
Network segmentation	Isolating IoT devices from critical systems	72% lower exposure
DNS filtering	Using secure resolvers (e.g., Cloudflare 1.1.1.1)	65% botnet domains blocked (APNIC, 2020)
Intrusion detection	Tools like Snort/Suricata for traffic analysis	89% success rate

Since average users often lack the technical expertise to detect or prevent their devices from being involuntarily used in Distributed Denial of Service (DDoS) or Distributed Reflective Denial of Service (DRDoS) attacks, the responsibility for cybersecurity must be distributed across key stakeholders. Manufacturers are tasked with improving security practices by designing safer software and accelerating the release of critical patches. ISPs should take an active role in monitoring network traffic and blocking botnet activity before it escalates. Meanwhile, governments must enforce user education initiatives and establish clear regulatory frameworks that promote cooperation between the public and private sectors. This combined, multi-stakeholder approach offers a more resilient and effective defense against the growing global threat of DDoS and DRDoS attacks, reducing both the frequency and impact of such incidents.

ETHICAL AND SOCIAL RESPONSIBILITY IN CYBERSECURITY

Cybersecurity is not merely an individual concern but a collective responsibility. States and educational systems should promote cyber hygiene through mandatory school curricula and public awareness campaigns.

The Collective Nature of Cybersecurity

Cybersecurity has evolved into both a societal and ethical imperative. As digital integration continues to deepen, maintaining cyber hygiene has become a public good, much like clean water or road safety. Several compelling arguments support the notion of shared responsibility for cybersecurity. First, the "tragedy of the commons" suggests that individual negligence can jeopardize entire networks, as insecure devices can become vectors for widespread harm (Schneier, 2018). Second, network effects highlight that a single unsecured device can be exploited to launch attacks on critical infrastructure, amplifying the consequences of individual inaction (Clark & Knake, 2019). Lastly, the concept of asymmetric consequences points out that users rarely bear the full costs of the harm caused by their compromised devices, leaving others to shoulder the burden (Anderson et al., 2020). Together, these arguments reinforce the need for a collective approach to cybersecurity, where shared responsibility is essential for protecting the broader digital ecosystem.

The State's Role in Promoting Cyber Culture

Educational Reforms

Systemic education from childhood shapes security habits most effectively (Livingstone et al., 2021):

Country	Program	Content	Impact
Estonia	ProgeTiiger (2012)	Mandatory coding/ cybersecurity in schools	72% of students recognize threats (TalTech, 2022)
Japan	Cyber Colosseo	Gamified malware education	40% fewer youth infections (NISC, 2023)
U.S.	CYBER.ORG (K-12)	Standardized teacher resources	Adopted in 48 states (DHS, 2023)

B) Public Campaigns

UK's Cyber Aware: Increased 2FA usage from 32% to 61% (NCSC, 2022).
EU's No More Ransom: Reduced ransomware payments by 53% (Europol, 2023).

ETHICAL FRAMEWORKS FOR CORPORATE RESPONSIBILITY

Under the principle of Duty of Care, tech companies are obligated to take proactive steps to ensure the security and safety of their products. This includes designing secure products from the outset, adhering to principles like Privacy by Design as outlined in ISO 31700, and ensuring that their software is resilient to threats. Additionally, companies are expected to disclose vulnerabilities transparently, following standards such as the Common Vulnerabilities and Exposures (CVE) system, to help the wider security community address risks promptly. Furthermore, tech companies must adapt user interfaces to accommodate non-technical users, making security features more accessible and understandable (Whitten & Tygar, 1999).

However, controversies surround this issue. One key concern is the tendency to blame users for security breaches, often shifting responsibility away from manufacturers to end-users, even though many users lack the knowledge or resources to protect themselves adequately (Reeder et al., 2022). Another challenge is digital inequality, where poorer populations may lack access to the necessary security tools and technologies, exacerbating the vulnerability gap and leaving them exposed to cyber risks (UNCTAD, 2022). These issues highlight the complexity of assigning responsibilities and the need for a more equitable and holistic approach to cybersecurity.

DISCUSSION

An analysis of the legal, technical, and ethical dimensions of involuntary participation in cyberattacks reveals that responsibility in the digital space cannot be understood through a single disciplinary lens. Instead, it emerges as a multilayered and interdependent concept, shaped by the interaction of regulatory frameworks, technological design, and user behavior. This chapter synthesizes the findings and compares the different approaches to liability, highlighting both the convergences and tensions.

DIVERGENT UNDERSTANDINGS OF RESPONSIBILITY

The legal, technical, and ethical perspectives examined in this work approach responsibility from fundamentally different starting points:

- Legal frameworks focus on assigning liability and determining whether a user acts negligently or intentionally. They rely on established concepts such as due diligence, foreseeability, and duty of care.

- Technical analyses emphasize systemic vulnerabilities and the structural nature of cyber risks. From this perspective, responsibility is distributed across the entire digital ecosystem, including manufacturers, service providers, and network operators.

- Ethical perspectives highlight moral expectations and the realistic capacities of users. They question whether it is fair to hold individuals accountable for risks they cannot fully understand or control.

These differences illustrate why debates about user liability remain unresolved: each domain defines responsibility according to its own logic and priority.

SHARED RESPONSIBILITY AS AN EMERGING PARADIGM

Despite their differences, the three perspectives converge on one central insight: responsibility in the digital space is shared. No single actor—neither the user, the manufacturer, nor the state—can independently ensure cybersecurity. Instead, effective protection requires coordinated action:

- Users must follow basic security practices.

- Manufacturers must implement secure by design principles.

- Service providers must detect and mitigate such malicious traffic.

- Regulators must establish enforceable standards and incentives.

This shared responsibility model aligns with broader trends in cybersecurity governance, where the complexity of digital systems makes individual accountability insufficient on its own.

TENSIONS BETWEEN USER EXPECTATIONS AND SYSTEMIC REALITIES

The comparison of perspectives also reveals several persistent tensions:

- Knowledge asymmetry: Users are expected to maintain secure devices, yet many lack the expertise to do so effectively.

- Control asymmetry: Manufacturers and service providers control most security relevant features, but users often bear the consequences of failures.

- Regulatory asymmetry: Legal frameworks evolve slowly, while cyber threats evolve rapidly, creating gaps between regulation and reality.

These tensions suggest that holding users legally responsible for involuntary participation in cyberattacks may be both impractical and ethically questionable unless broader systemic reforms are implemented.

IMPLICATIONS FOR POLICY AND PRACTICE

The synthesis of findings points to several implications:

- Legal reforms should clarify the boundaries of user responsibility while placing greater obligations on actors with actual control over device security.

- Technical measures such as automated updates, secure defaults, and network level filtering can significantly reduce the burden on users.

- Ethical considerations call for realistic expectations of user behavior and emphasize the importance of digital literacy initiatives.

Together, these implications support a more balanced and equitable approach to cybersecurity responsibility—one that recognizes the interconnected nature of digital systems.

FUTURE DIRECTIONS: FROM "CYBER HYGIENE" TO "CYBER CITIZENSHIP"

Emerging concepts in cybersecurity advocate for a more collaborative and comprehensive approach to protecting the digital ecosystem. One such concept is digital subsidiarity, which emphasizes shared responsibility among individuals, corporations, and states, highlighting the need for collective action to address cybersecurity challenges (Maras, 2016). In addition to this, regulatory innovations are gaining traction. For example, the Cybersecurity VAT, a proposed tax on insecure Internet of Things (IoT) devices by ENISA in 2023, aims to incentivize manufacturers to prioritize security. Another innovative idea is cyber immunization, which likens preventive measures in cybersecurity to vaccination, offering a proactive approach to defense.

Addressing the ethical and social dimensions of cybersecurity calls for systemic approaches. Schools, for instance, must integrate digital literacy into their core curriculum to equip future generations with essential skills. Policies should strike a balance between regulation and incentives, encouraging compliance while fostering innovation. Moreover, corporate ethics must go beyond merely meeting legal requirements, embracing a culture of responsibility and proactive action.

The concept of cyber citizenship provides a sustainable framework for shared responsibility, wherein individuals, organizations, and governments play their part in fostering a secure digital environment. This holistic approach ensures that cybersecurity is not only a technical concern but also a societal obligation.

CONCLUSION

This research demonstrates that responsibility for Distributed Denial of Service (DDoS) and Distributed Reflective Denial of Service (DRDoS) attacks cannot rest solely on individuals. Instead, it requires a holistic approach that integrates legal, technical, and ethical measures to address the complexities of cybersecurity.

The key findings emphasize the need for legal frameworks that strike a balance between protecting uninformed users and penalizing gross negligence. For example, the EU's NIS2 Directive and the U.S. CFAA aim to safeguard users who may not be aware of security threats, while also holding individuals and organizations accountable for negligent behaviors that contribute to cyberattacks. On the technical front, solutions such as automatic software updates (e.g., Microsoft's Windows updates, 2023), ISP-based botnet detection systems (van Rijswijk-Deij, 2016), and user-friendly security interfaces (Whitten & Tygar, 1999) are essential for reducing vulnerabilities and empowering users to protect their devices.

From an ethical perspective, societal initiatives like Estonia's ProgeTiiger educational program and the UK's Cyber Aware campaigns are crucial in fostering a culture of cybersecurity awareness and shared responsibility.

Looking forward, future directions in cybersecurity will likely focus on the concept of cyber citizenship (Maras, 2016), which promotes collective responsibility, and on regulatory innovations such as IoT security taxes to incentivize secure product development. Combining these innovations with technological advancements and continuous educational efforts will be key to building sustainable cyber resilience and ensuring a safer digital future for all.

REFERENCES

Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). Wiley.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., Zhou, Y., & Zhao, Y. (2017). Understanding the Mirai botnet. In Proceedings of the 26th USENIX Security Symposium (pp. 1093–1110). USENIX Association. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

APNIC. (2020). DNS security best current practices. https://www.apnic.net

Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Praeger.

Christen, M., Gordijn, B., & Loi, M. (Eds.). (2020). The ethics of cybersecurity. Springer.

CISA. (2022). Shields Up: Guidance for organizations. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/shields-up

Clark, R. M., & Knake, R. (2019). The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats. Penguin Press.

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention) (ETS No. 185). https://www.coe.int/en/web/cybercrime

Dainotti, A., Benson, K., King, A., et al. (2017). Analysis of country-wide internet outages caused by censorship. In Proceedings of the ACM Internet Measurement Conference (IMC).

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). (2022). Official Journal of the European Union.

European Union. (2016). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). Official Journal of the European Union.

Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. International Telecommunication Union.

Google Project Zero. (2021). A 2021 review of 0 day exploits in the wild. Google Security Blog. https://googleprojectzero.blogspot.com

Hardin, G. (1968). The tragedy of the commons. Science, 162(3859), 1243–1248.

Home Office. (2023). Review of the Computer Misuse Act 1990: Consultation response. UK Home Office.

Kerr, O. S. (2018). Computer crime law (4th ed.). West Academic.

Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80–84. https://doi.org/10.1109/MC.2017.201

Maras, M.-H. (2016). Cybercriminology. Oxford University Press.

Microsoft. (2023). Microsoft Security Update Guide. Microsoft Security Response Center. https://msrc.microsoft.com/update-guide

Schjolberg, S. (2017). The history of cybercrime: 1976–2016. Books on Demand.

Schneier, B. (2018). Click here to kill everybody: Security and survival in a hyper-connected world. W. W. Norton.

Sengupta, S., Chowdhury, N., & Huang, D. (2021). A survey of DDoS attacks and defense mechanisms. ACM Computing Surveys, 54(7), Article 152.

United States Congress. (1986). Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

United States v. Nosal, 844 F.3d 1024 (9th Cir. 2016).

Van Rijswijk-Deij, R., Sperotto, A., & Pras, A. (2016). DNSSEC and its potential for DDoS attacks. In Proceedings of the ACM Internet Measurement Conference (IMC).

Wall, D. S. (2024). Cybercrime: The transformation of crime in the information age (2nd ed.). Polity Press.

Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In Proceedings of the 8th USENIX Security Symposium.

Woods, D., & Simpson, A. (2017). Policy measures and cyber security: Secure by design. Journal of Cyber Policy, 2(2), 209–226. https://doi.org/10.1080/23738871.2017.1360927

World Economic Forum. (2022). Global cybersecurity outlook 2022. https://www.weforum.org

Zengupta, S., Chakraborty, S., & Das, S. K. (2021). A comprehensive survey on DDoS attacks and defense mechanisms. Computer Science Review, 40, 100364. https://doi.org/10.1016/j.cosrev.2021.100364

Zetter, K. (2014). Countdown to zero day: Stuxnet and the launch of the world's first digital weapon. Crown.

Media, Culture and Public Relations Vol.17, 1

INFO - 200

https://doi.org/10.63191/mcpr.17.1.2

PRAVNA I ETIČKA ODGOVORNOST KOD NESVJESNOG SUDJELOVANJA U DDOS/DRDOS NAPADIMA

Krunoslav Antoliš

SAŽETAK: Digitalno okruženje postaje sve složenije, a kibernetički napadi poput DDoS-a i DRDoS-a predstavljaju ozbiljnu prijetnju kritičnoj infrastrukturi, korporacijama i pojedincima (Zengupta i sur., 2021.). Ključno pitanje u tom kontekstu jest pitanje odgovornosti u situacijama kada vlasnik računala nije svjestan da je njegov uređaj kompromitiran i da se koristi za pokretanje napada. Ovaj rad analizira pravne, tehničke i etičke aspekte odgovornosti u digitalnom prostoru kroz tri istraživačka pitanja: (1) kako pravni okviri tretiraju odgovornost vlasnika u slučajevima neznanja, (2) koje tehničke mjere mogu spriječiti nenamjerno sudjelovanje u napadima te (3) postoji li etička obveza društva da educira korisnike.

Metodološki pristup obuhvaća kvalitativnu analizu literature, pravnih dokumenata (direktiva EU-a NIS2, američki zakon CFAA), studija slučaja (botnet Mirai) i stručnih radova iz područja kibernetičke sigurnosti. Rezultati pokazuju da većina pravnih sustava ne kažnjava korisnike koji nisu svjesni zaraze, osim ako nisu pokazali grubu nepažnju (Schjolberg, 2017.). Ipak, tehnička nespremnost korisnika nalaže preraspodjelu odgovornosti prema proizvođačima softvera, pružateljima internetskih usluga (ISP-ovima) i državnim tijelima. Etička analiza naglašava kolektivnu prirodu kibernetičke sigurnosti i potrebu za sustavnom edukacijom (Livingstone i sur., 2021.).

KLJUČNE RIJEČI: odgovornost za kibernetičku sigurnost, DDoS/DRDoS napadi, uključenost botneta, pravni i etički okviri, model zajedničke odgovornosti