

# A Novel Cybersecurity Ethical Maturity Model Based on AHP Method

Cevat Özarpa<sup>1</sup>, İsa Avcı<sup>2</sup>, Yahya Zakrya Khan<sup>2\*</sup>

<sup>1</sup>Faculty of Engineering and Natural Sciences, Department of Biomedical Engineering, Ankara Medipol University, Ankara, Türkiye, <https://ror.org/01c9cnw16>

<sup>2</sup>Department of Computer Engineering, Karabük University, Karabük, Türkiye, <https://ror.org/04wy7gp54>

Corresponding author:

Yahya Zakrya Khan, Karabük University,  
Faculty of Engineering,  
Department of Computer  
Engineering, Karabük, Türkiye  
2528127501@ogrenci.karabuk.edu.tr

## ABSTRACT

This study uses the Analytic Hierarchy Process (AHP) method to evaluate the importance of ethical values in the cybersecurity profession and to measure ethical maturity. In a study with 37 cybersecurity professionals from Türkiye, 27 ethical values were organized based on international ethical standards, including those of the ACM, IEEE, ISACA, (ISC)<sup>2</sup>, NIST, and the UK Cyber Security Council. The AHP analysis identified Confidentiality and Privacy, Awareness of Responsibility, and Cyber Sovereignty and Independence Ethics as the most vital values, representing 11.98% of the total. Conversely, values such as Transparency, Respect for Cultural Diversity, and Traceability were considered less important. The study also introduced a new Cybersecurity Ethical Maturity Model, outlining ethical development across five stages, and compared this model with selected cyber incidents in Türkiye. It highlights the effect of ethical violations on public trust and offers recommendations for policy and training strategies. Overall, the study contributes a unique, quantitative ethical assessment tool aligned with international standards and provides a strategic framework for fostering a sustainable digital security culture.

**Keywords:** Cybersecurity, Cyber ethical values, Analytic Hierarchy Process (AHP), Ethical Maturity Model, Privacy and Confidentiality

## Article History:

Received: 03.07.2025

Revised: 22.10.2025

Accepted: 02.11.2025

Published Online: 11.12.2025

## 1. Introduction

Ethics are the basic moral principles that help individuals to distinguish between right and wrong. With its philosophical history dating back to Ancient Greece, it has evolved into an interdisciplinary field that systematically examines the value judgments of individuals. Ethics refers not only to individual conscience but also to a collective structure based on social trust, justice, and responsibility. While Aristotle's virtue ethics centers on the individual's character development, Kant's deontological approach defines acting in accordance with universal rules as a moral obligation [1], [2].

Ethics has vital importance not only at the individual or philosophical level but also in organizational structures and professional fields in the 21st century. Especially in areas that require high responsibility, such as technology, informatics, and security, ethical values are among the determining factors that directly affect decision-making processes [3]. In this context, cybersecurity is not only a technical discipline but also a multi-dimensional area of expertise that involves serious ethical responsibilities. Cybersecurity is a set of policies and practices designed to protect information systems, digital data, and technological infrastructures against unauthorized access, use, disclosure, corruption, or destruction. This process extends beyond software and hardware measures, encompassing various components, including human factors, regulatory frameworks, and, most notably, ethical approaches. The growing complexity of cyber threats demonstrates that sustainable security cannot be achieved solely through technical measures. Ethical weaknesses in human behavior often lead to incidents such as ransomware, phishing attacks, and social engineering. This situation necessitates that cybersecurity be supported by ethical awareness, individual responsibility, social sensitivity, and technical capacity.

Ethical principles contribute to the creation of secure digital environments at both individual and organizational levels through values such as confidentiality, data integrity, fairness, transparency, and accountability [4]. The ACM Code of Ethics recommends designing systems that are not only functional but also consider ethical responsibility [5]. Similarly, organizations such as (ISC)<sup>2</sup>, ISACA, and NIST expect cybersecurity professionals to adopt high ethical standards in areas such as public safety, integrity, individual privacy, and compliance with the law [6], [7], [8]. For instance, ISACA's certification programs, such as CISA, CISM, and CRISC, require experts to have not only technical knowledge but also ethical behavior principles [7]. The NIST Cybersecurity Framework, on the other hand, does not provide a direct code of ethics, but supports a culture of cyber risk management within the framework of principles such as confidentiality,

transparency, accountability, and fairness. The guidance published by the UK Cyber Security Council (UK CSC) also encourages the integration of common ethical behavior principles that prioritize professionalism, equality, and public interest into professional practices [9], [10].

The cybersecurity profession has a structure that requires high ethical awareness and understanding of responsibility, as well as technical competence. Professionals working in tasks such as protecting user data, system security, and preventing unauthorized access are obliged to comply with high ethical standards. This obligation has been institutionalized by the principles of non-maleficence, respect for confidentiality, and the public interest, as set forth by organizations such as IEEE [11].

The integration of ethical values into vocational practices and normative ethical theories also provides a crucial theoretical foundation for this approach. Deontological, utilitarian, and virtue ethics approaches provide universal principles to guide individuals' decision-making processes [1], [2]. These theories guide the solving of ethical dilemmas faced by professionals, especially in complex and multi-stakeholder cybersecurity environments.

Therefore, ethical awareness stands out as a key component of sustainable digital security, given that ethical violations can lead not only to technical vulnerabilities but also to a loss of social trust. Professional awareness should go beyond the individual level and be integrated into organizational strategies, security policies, and professional standards. Ethical responsibility is a strategic requirement that needs to be continuously developed not only on an individual basis but also on an organizational and societal level.

## 1.1. Theoretical Framework

### 1.1.1. The Concept of Maturity

Maturity is a critical concept that expresses the level of development of individuals or organizations in a particular field, as well as the extent to which their processes are structured, measurable, and sustainable. This concept offers the opportunity to assess not only the current state of organizational capacity but also its potential for future development. The People Capability Maturity Model (People CMM), one of the most frequently referenced models in the literature, enables the systematic analysis of processes and the identification of development steps. Such models are widely used, especially in human resource management and in measuring the maturity level of organizational structures. Structures with a high level of maturity are more flexible, resilient, and capable of making strategic decisions in the face of uncertainties and threats. Therefore, maturity level should be considered as an indirect indicator not only of operational competence but also of dimensions such as strategic management, organizational resilience, and ethical integrity [12].

### 1.1.2. Importance of Ethical Value Analysis with AHP

In multi-stakeholder, rapidly changing, and high-risk areas such as cybersecurity, there is a critical need to analyze decision-making processes based on ethical values with objective and systematic methods. In this context, the Analytic Hierarchy Process (AHP) method is a structured and numerically based evaluation tool that stands out among multi-criteria decision-making (MCDM) approaches. AHP enables decision-makers to rank various ethical values in order of comparative importance. With this method, ethical dilemmas can be analyzed within the framework of hierarchical structures; individual attitudes and value judgements can be transformed into measurable data [13], [14]. Analyzing ethical values with AHP enables not only the measurement of individual awareness but also the evaluation of professional and institutional ethical maturity. In this way, the similarities and differences between the ethical priorities of various expert groups can be objectively compared and analyzed. It also provides valuable input for organizational decision-making mechanisms such as human resources management, recruitment processes, professional competence assessments, and ethics training planning. Thus, AHP is not only a technical analysis tool but also a methodological framework to guide ethics-oriented strategic planning. In this study, the prioritization results obtained by the AHP method are analyzed comparatively with selected cybersecurity incidents in Türkiye in recent years. Furthermore, a cybersecurity ethical maturity model is presented in Section 3.

## 2. Literature Review

In recent years, there has been a significant increase in studies examining the application of ethical principles in cybersecurity and their relationship to professional competence. In this context, various theoretical and practical approaches that focus on individuals' attitudes influenced by ethical value systems, levels of professional development, and behavioral patterns in decision-making emerge prominently. The literature particularly examines how ethical theories influence individual decisions, how maturity models depict organizational capacity, and how ethical decision-making processes impact digital security practices. This section begins by discussing maturity models and then explores current approaches to ethical decision-making in cybersecurity.

### 2.1. Maturity Models

In today's cybersecurity landscape, technical measures alone are not enough; decision-making frameworks based on ethical principles are essential for maintaining secure digital infrastructures. Maturity models created within this context are no longer solely focused on measuring technical capabilities; they have evolved into multi-dimensional evaluation tools that

incorporate ethical awareness, organizational responsibility, and individual consciousness. Below, key models that consider ethical awareness are discussed, and the roles of these frameworks are analyzed.

One significant institutional level is the Cybersecurity Maturity Model for the Protection and Privacy of Personal Health Data presented by Rojas et al. (2022). This structure, based on the C2M2 architecture of the US Department of Energy, is adapted for the Peruvian health sector and measures the maturity level on the axes of cybersecurity, privacy, and personal health data management through a total of 10 areas, 29 objectives, and 317 implementation criteria. The findings indicate low levels of maturity, particularly in areas such as access control, human resource competence, and system architecture, as well as partial progress in risk and threat management. The model opens the door to applications based on an ethical framework, centering on the privacy of individuals [15].

Complementing this institutional perspective, David (2022), with 21 cybersecurity professionals working in the defense industry. In this grounded theory study, ethical tensions were analyzed around values such as autonomy, usefulness, prudence, and accountability based on stakeholder theory. The study revealed that, beyond technical competence, compliance with organizational ethical codes, transparent communication, and continuous ethical training have a direct impact on the maturity level. In this respect, the model shows that organizational ethical awareness is much more than just a written policy [16].

At the individual level, Sadeghi et al. (2023) created a serious game-based training scenario in their study, based on five basic ethical principles (beneficence, nonmaleficence, fairness, autonomy, and explainability), and modeled the moral preferences of 250 cybersecurity students using the decision tree method. The findings indicate that an individual's cultural background, extroversion, sense of responsibility, and sense of belonging influence their ethical preferences. This study offers valuable insights into how personalized education models can be integrated into ethical maturity strategies [17].

Extending the discussion to a community-level framework, the Community Cyber Security Maturity Model (CCSMM) was developed by Sjin et al. (2016). The model presents a five-stage development process (Awareness, Initial, Structured, Institutionalized, and Dynamic) and enables the measurement of leadership, communication, public relations, social and ethical awareness, and technical capacity. It aims to create a collective safety culture by encouraging the active participation of local governments and non-governmental organizations in the processes [18].

Finally, a comparative analysis of all these models was carried out by Rea-Guaman et al. (2017). The research evaluated widely used cybersecurity maturity models, including C2M2, NIST CSF, CERT-RMM, and COBIT, in both structural and functional dimensions. Although it is stated that NIST and C2M2 models offer advantages in terms of flexibility and measurability, it is emphasized that these models do not directly include ethical values. This situation highlights the need to develop new-generation maturity models with an ethical focus [19].

In developing a cybersecurity maturity framework specific to Türkiye, it is essential to consider national standards and regulatory mechanisms that shape institutional information security practices. Two key references underpin Türkiye's cybersecurity governance: the ISO/IEC 27001:2022 standard, adopted as TS EN ISO/IEC 27001 within the Information Security Management System (ISMS) framework [20], [21], and the Information and Communication Security Guide (BİGR) issued by the Presidential Digital Transformation Office [22], [23].

The ISO/IEC 27001:2022 standard restructures its Annex A control catalogue into 93 controls grouped under four domains (organizational, human, physical, and technological), explicitly addressing ethical considerations in cybersecurity management, such as access governance, incident handling, monitoring, and accountability. Complementing this international framework, the BİGR provides a nationally harmonized reference model defining minimum mandatory measures and auditing mechanisms for public institutions and critical infrastructure operators. Introduced through Presidential Circular No. 2019/12 [22] and reinforced by the Information and Communication Security Audit Guide (2021) [23], this approach institutionalizes a systematic auditing process, thereby strengthening ethical compliance and organizational responsibility.

The ethical maturity model proposed in this study establishes a conceptual linkage between these national frameworks and ethical value dimensions. Through comparative mapping of the model's ethical components with the ISO/IEC 27001 Annex A control families and the operational domains of BİGR, the study demonstrates how values such as privacy, accountability, transparency, and responsibility awareness are embedded into institutional cybersecurity processes. Furthermore, the National Cybersecurity Strategy and Action Plan (2024-2028) [24] reinforces this alignment by emphasizing continuous BİGR compliance, institutionalization of independent audits, and capacity-building initiatives aimed at enhancing ethical and organizational maturity across Türkiye's cybersecurity ecosystem.

Most existing models prioritize technical capacity, process management, and operational standards, while a direct, holistic, and measurable assessment structure for ethical values remains secondary, as shown in Table 1. This underscores the need for new-generation maturity approaches that focus not only on technological aspects but also on the human and ethical dimensions of cybersecurity.

Table 1. Comparison of Ethical Maturity Models.

Study	Reference	Scope & Level	Key Features	Major Results / Contributions
Cybersecurity Maturity Model for the Protection and Privacy of Personal Health Data	[15]	Institution, Health sector	C2M2-based, 3 axes (cyber security, privacy), 10 areas, 29 targets, 317 applications	There is a need for ethics-oriented development in areas with low maturity, such as privacy and access control.
An Ethical Framework for Cybersecurity Professionals: A Grounded Theory Study	[16]	Institution, Expert experience	Qualitative interviews with 21 experts, based on stakeholder theory (autonomy, usefulness, accountability)	Ethical awareness, code compliance, and continuous training are determinants of corporate maturity.
Modelling the ethical priorities influencing decision-making in cybersecurity contexts.	[17]	Individual, Student	250 students, decision trees, and a severe game scenario based on 5 ethical principles	Individual characteristics influence ethical preferences and the need for personalized education.
The Community Cyber Security Maturity Model	[18]	Community / Local authority	5 levels (Awareness, Dynamic), leadership, public relations, and social ethical awareness	Building collective ethical awareness and community-based safety culture.
Comparative study of cybersecurity capability maturity models	[19]	Model Comparison	C2M2, NIST CSF, CERT-RMM, COBIT comparison, structural and functional analysis	The lack of an ethical dimension is evident, and it is a necessity for new generation models based on ethics.
ISO/IEC 27001:2022 - Information Security Management Systems	[20], [21]	Standard / Institutional governance	Annex A: 93 controls under four themes (organizational, people, physical, technological)	Aligns access control, monitoring, incident response, and accountability processes with ethical values and governance.
Information and Communication Security Guide (BiGR) & Audit Guide (2021)	[22], [23]	National policy / Public sector & critical infrastructure	Presidential Circular 2019/12 mandates minimum measures; national audit methodology (annual, independent planning/execution/reporting, results to DDO)	Institutionalizes auditing; reinforces ethical compliance, transparency, and accountability across the public sector & critical infrastructure.
National Cybersecurity Strategy and Action Plan (2024-2028)	[24]	National strategy / Ecosystem	Recognizes BiGR & Audit Guide; sets monitoring & evaluation processes; capacity-building priorities	Strengthens ecosystem-level ethical and organizational maturity via sustained compliance and capability development.

## 2.2. Ethical Decision-Making Processes in Cybersecurity

Cybersecurity is a multi-layered discipline that encompasses not only technical measures but also decision-making mechanisms grounded in ethical values. Ethical sensitivity has a wide range of effects, from the daily behavior of individuals to the creation of corporate security policies, and directly shapes decision-making processes.

Within this scope, the ethical decision-making framework developed by Formosa et al. (2021), based on the ‘principlism’ approach, provides an important theoretical foundation for analyzing the dilemmas faced by cybersecurity professionals. The model is centered on the principles of beneficence, non-maleficence, autonomy, justice, and explicability, allowing for a context-sensitive evaluation of ethical issues that arise in various areas, from ransomware to penetration testing.

The fact that the model is grounded in multiple ethical principles rather than a single theoretical approach enhances its flexible applicability in the field. It supports the development of ethical capacity at both individual and organizational levels [25].

Building upon this, the study conducted by Flechais et al. (2023) shows that existing ethical codes do not adequately cover the problems encountered in practice. Based on the CyBOK framework, semi-structured interviews revealed a total of 122 ethical principles on issues such as exposure to illegal content, protecting customer privacy, and clarifying the boundaries of

professional responsibility. The study reveals that the ethical tensions frequently encountered in the field cannot be fully resolved by existing codes, and therefore emphasizes the need for clearer, functional, and adaptable ethical guidelines tailored to professional practice [26].

Further contributing to this discourse, Nasir et al. (2024) provide a comprehensive perspective on how ethical awareness can be internalized at the organizational policy level. The study examines the ethical dilemmas faced by cybersecurity experts through a multidimensional approach, addressing critical issues such as data privacy, informed consent, algorithmic bias, accountability, and the ethics of hacking. In particular, the case studies presented under the headings of security-privacy balance, transparency of user consent, and clear definition of corporate responsibility for data breaches reveal that ethical sensitivity should be integrated not only with individual awareness but also with corporate strategies. In this respect, the study contributes to both the theoretical foundations and practical implications of ethical decision-making processes in cybersecurity [27].

Adding a psychological dimension to the understanding of decision-making in cybersecurity, another important study was conducted by Al-Hashem et al. (2024). This research investigates how individuals perceive cyber threats and how they make decisions in response to these threats, within the framework of cognitive processes. Empirical findings reveal that media influence, personal experience, and organizational culture directly shape threat perception. Additionally, cognitive biases and risk perception were found to play a significant role in ethical decision-making processes. The study argues that awareness training should be supported not only with technical skills but also with psychological approaches, and ethical maturity strategies should be structured following personal psychological profiles [28].

Finally, from a normative standpoint, Navdeep et al. (2022) present another study that addresses the role of ethical principles in the development of cybersecurity policies. The research emphasizes that security measures should not be limited to technical competence but should also be structured with an ethical understanding that maintains a delicate balance between individual privacy, surveillance, and national security. The study argues that within the framework of the principle of 'not harm', not only individuals but also all segments of society should be protected by ethical security policies. It is also stated that policymakers should holistically address the new risks posed by artificial intelligence, IoT, and quantum technologies in the ethical context. In this context, it is stated that structures should be established where decision-makers can receive support from philosophical and social perspectives, as well as technical expertise [29].

Table 2. Comparison of Selected Studies Contributing to Ethical Decision-Making Processes in Cybersecurity.

Reference	Focus Point	Key Contribution
[25]	Principlism-based ethical decision framework	Context-sensitive solution proposal with multiple principles in ethical decision-making processes
[26]	Field inadequacies of ethical codes and the need for restructuring	Proposal for clear, actionable guidance for ethical tensions encountered in the field
[27]	Ethical hacking, data privacy, and organizational policies	250 students, decision trees, and a severe game scenario based on 5 ethical principles
[28]	Cognitive processes and the impact of threat perception on decision-making	Integration of threat perception and risk awareness into ethical education
[29]	Policy development with normative ethical principles (not harm, balance)	Integration of the ethical tenets into technical policy development processes

In general, the reviewed studies reveal that ethical awareness is not only a virtue for the cybersecurity profession but also a necessary component for sustainability and public trust. Ethical dilemmas in areas such as personal data security, organizational accountability, the limits of intervention, and the duty of disclosure require professionals to be guided by both their individual conscience and organizational values. Therefore, cybersecurity should be carried out by individuals who have not only technical skills but also value-oriented decision-making competencies based on ethical principles.

## 2.2. Classification of Ethical Values and Code Compliance

The classification of ethical values is structured based on nationally and internationally recognized professional ethical codes. In this context, each ethical value is based on the principles published by organizations such as ACM (Association for Computing Machinery), IEEE (Institute of Electrical and Electronics Engineers), (ISC)<sup>2</sup>, ISACA, NIST, and UK Cyber Security Council [5-11]. This mapping both strengthens the theoretical and practical validity of ethical values and provides a methodological basis for integrating ethical awareness into organizational practices. Moreover, it provides a structure that

is open to comparative analyses by ensuring that the assessment is meaningful not only in a local but also in a global context. Table 3 below shows the compliance of ethical values with international ethical codes.

Table 3. Compliance of Ethical Values with International Ethical Codes.

Ethical Value	ACM	IEEE	(ISC) <sup>2</sup>	ISACA	NIST	UK CSC	Description
Honesty	✓	✓	✓	✓	✓	✓	Truthfulness, correctness, and non-misleading.
Impartiality and non-bias	✓	✓	✓	✓	•	•	Impartial decision-making, fairness, and avoidance of bias.
Privacy and Confidentiality	✓	✓	✓	✓	✓	✓	Respect for the confidentiality and privacy of personal and corporate information.
Accountability	✓	✓	✓	✓	✓	✓	Responsibility to take ownership and accountability for the consequences of their behavior.
Awareness of Responsibility	✓	✓	✓	✓	✓	✓	Acting with awareness of duties and roles, recognizing ethical obligations.
Commitment to the Law	✓	✓	✓	✓	✓	✓	Compliance with applicable laws, regulations, and ethical standards.
Transparency	✓	✓	✓	✓	✓	•	Open, honest, and understandable sharing of information.
Respect and Co-operation	✓	✓	✓	✓	•	✓	Respect and cooperate with colleagues, stakeholders, and the community.
Professionalism	✓	✓	✓	✓	✓	✓	Technical qualification, continuous improvement, and professional ethical behavior.
Ethical Leadership	✓	✓	✓	✓	•	•	Promoting ethical culture and setting an example for colleagues.
Innovative Learning	✓	✓	✓	✓	✓	✓	Openness to new knowledge and willingness to learn continuously.
Social Responsibility	✓	✓	✓	✓	•	✓	Sensitivity to society, the individual, and corporate social responsibility.
Justice and Equality	✓	✓	✓	✓	•	✓	Equal treatment of all individuals and fair practices.
Environmental Responsibility	✓	✓	•	✓	•	•	Environmentally sensitive practices and sustainability awareness.

Table 3(Continued)							
Security Awareness	✓	✓	✓	✓	✓	✓	Sensitivity and defense awareness against information security threats.
Responsible Disclosure and Notification	✓	✓	✓	✓	✓	✓	Disclosure and reporting of unethical situations through appropriate means.
Avoiding Unauthorized Intervention	✓	✓	✓	✓	✓	✓	Avoiding unauthorized access and interference.
Data Ownership	✓	✓	✓	✓	✓	✓	Respect for the rights of individuals over their personal data.
Influence Analyses	✓	✓	✓	✓	✓	✓	Evaluating the potential consequences of ethical practices.
Traceability	✓	✓	✓	✓	✓	✓	All actions are traceable and transparent.
Accessibility	✓	✓	✓	✓	✓	✓	Ensuring everyone's access to information and systems.
Respect for Cultural Diversity	✓	✓	✓	•	•	✓	Respectful approach to different cultures and traditions.
Awareness of Homeland and Public Service	•	✓	✓	✓	✓	✓	Service understanding prioritizes the needs of society and the public interest.
National Security Sensitivity	•	✓	✓	✓	✓	✓	Sensitivity to and defense of the country's digital security and sovereignty.
Respect for Public Resources	✓	✓	✓	✓	✓	✓	Effective, efficient, and honest use of public resources.
Prioritization of Community Benefits	✓	✓	✓	✓	✓	✓	Prioritizing the public good over individual interests.
Cyber Sovereignty and Independence Ethics	•	•	•	✓	✓	✓	Technological sovereignty and national cyber security awareness.

\*\*Note: (Implicitly = •), this value is not directly named but is implied by statements or expectations of behavior.

### 2.3. Case Study Analyses from Türkiye: Evaluation in Line with Ethical Values

To establish a contextual foundation for the development of the proposed maturity model, this section provides a critical analysis of major cybersecurity incidents that have occurred in Türkiye from an ethical standpoint. Rather than serving as empirical validation, these cases function as illustrative examples demonstrating how ethical priorities and deficiencies are manifested within the practical realities of national cybersecurity practices.

Cyberattacks against public institutions in Türkiye have been increasing significantly in recent years. In 2015, Distributed Denial of Service (DDoS) attacks against Türk Telekom and several banks resulted in service interruptions, threatening the continuity of public services. Similarly, targeting Ministry of Health data during the COVID-19 pandemic, which emerged in 2020, revealed the vulnerability of critical infrastructures to cyber threats. Despite initiatives such as the National Cybersecurity Strategy and Action Plan, public systems still face attacks from both local and international sources [30]. Allegations of data leakage regarding the e-Devlet system sparked a serious public debate. In 2023, despite claims that the data of 85 million citizens had been stolen, the authorities stated that these claims were not technically feasible and that only user profile information was stored in the system. Similarly, technical analyses did not confirm data leaks alleged to have

occurred in 2021 through systems such as e-Nabız, EBA, and ÖSYM. It was determined that most of the incidents were caused by targeting users' individual accounts through phishing and malware. In this context, the importance of ethical values such as privacy and user awareness once again emerges [31].

Although Law No. 6698 on the Protection of Personal Data (KVKK) is essential for securing personal data in Türkiye, some corporate violations indicate that this legal framework is not being implemented effectively. In 2018, a data breach at a leading e-commerce platform allowed cyber attackers to capture user information and exposed security vulnerabilities. In 2022, an allegation surfaced that customer information of a major GSM operator had been leaked on the internet, sparking serious concerns among the public. The delays in Türkiye's data protection legislation have contributed to the occurrence of such violations. Convention No. 108, signed in 1981 but entering into force in 2016, clearly indicates that the legal infrastructure could not be established on time. In addition, incidents such as the leakage of voter data onto the internet during the 2009 local elections demonstrate that even public institutions have significant weaknesses in data security [32].

Cyberattacks have become an essential threat to the banking sector in Türkiye. In 2016, attacks on ATM systems resulted in significant financial losses; by 2021, phishing attempts via mobile banking and SMS had become more prevalent. Advanced techniques, such as 'Man-in-the-Browser' and 'Automated Transfer Systems', which enable unauthorized money transfers from users' accounts, were used in these attacks. In addition, credit card fraud has become widespread, with card copying and routing methods posing a serious threat to users' digital security. In this context, technical measures, user education, and ethical awareness should be systematically strengthened. To prevent unethical behaviors in the digital environment, it is essential to increase corporate responsibility and user-oriented ethical awareness in the banking sector [33].

Table 4. Selected Cybersecurity Cases from Türkiye and Their Correspondence to the Stages of the Cybersecurity Ethical Maturity Model (CEMM)

Year	Sector & Case	Featured Ethical Value(s)	Significant Vulnerability / Consequence	Relationship with Stage in the Model
2015	Telecom & Banking, Large-scale DDoS attacks	National Security Sensitivity, Awareness of Responsibility	Severe disruption, exposed national infrastructure weaknesses	Stage 2 Initiation: Reactive posture, absence of foundational policies
2018	E-commerce platform data leakage	Data Ownership, Commitment to the Law, Accountability	Violation of KVKK (Turkish Data Protection Law), millions of records leaked	Stage 3 Structured: Policies exist, but enforcement remains weak
2019-20	Targeting of the Ministry of Health data (COVID-19)	Privacy and Confidentiality, Awareness of Responsibility	Cyberattacks during the pandemic crisis, health data at risk	Stage 4 Integrated: Ethics integrated, but performance falters in crisis
2021	Mobile banking & SMS phishing	Honesty, Awareness of Responsibility	Financial scams, low user cyber awareness	Stage 3 Structured: Tools present, user awareness missing
2022	GSM operator customer data leakage	Data Ownership, Transparency, Accountability	User data exposed, breach notification delayed	Stage 2 Initiation: Legal base exists, communication is not transparent
2023	'85 million e-Devlet data leaked' allegation	Privacy and Confidentiality, Transparency	No confirmed breach, but high public mistrust and media amplification	Stage 1 Awareness: Public risk perception grew, but transparency was lacking
TürkNet(2025)	TürkNet customer leak	Privacy and Confidentiality, Accountability, Responsible Disclosure, and Notification	Customer PII (ID, phone number, address, and static IP) was exfiltrated; no passwords or financial data were leaked on illicit forums.	Stage 3 Structured: Controls exist, but disclosure accountability is weak.

\*\*Note: The classification of each case by maturity stage is based on the five-level Cybersecurity Ethical Maturity Model (CEMM) proposed in this study (see Fig. 3 in Section 3.3). Each stage reflects the organization's ethical development level, ranging from Stage 1: Awareness to Stage 5: Excellence, as applied to the contextual analysis of Türkiye's cybersecurity incidents.

Another crucial factor, alongside technical infrastructure, in cybersecurity is the level of awareness among individuals and organizations. Many organizations in Türkiye are vulnerable to digital threats due to their personnel's limited knowledge of cybersecurity. Although awareness in this field has increased in recent years, sustainable and comprehensive educational activities are still not widespread enough. Equipping public and private sector personnel with cybersecurity awareness is critical for the security of technical systems and understanding ethical responsibilities. Domestic software should be encouraged to overcome these deficiencies, and specialist training programs should be expanded [34], [35].

It has been observed that the focus on privacy and confidentiality, which has the highest rate in the AHP analysis, 11.98%, has a direct correspondence in the e-Devlet and TürkNet cases [36]. On the other hand, the inadequate implementation of awareness of responsibility and accountability in the field, particularly the lack of transparent reporting by organizations, aligns with the development areas identified in the maturity model. In conclusion, the proposed model has the potential to both explain the critical weaknesses in the cases and inform policy and training design [37].

This table illustrates that when highly valued ethical principles, such as confidentiality, privacy, and accountability, are compromised, the consequences tend to be severe and systemic, often impacting critical infrastructures and eroding public trust. In contrast, transparency and accountability are considered lower in the ethical maturity hierarchy but play a crucial role in effective crisis management and public perception. Their absence can significantly increase the impact of an incident, particularly in terms of undermining trust and delaying organizational response.

### 3. Materials and Methods

#### 3.1. Data Set and Survey Application

The data set of this study was created through a structured online survey conducted with the participation of cybersecurity professionals actively working in Türkiye. The study's primary purpose is to determine the individual priorities of the participants regarding ethical values and to analyze the relationship between these priorities and their professional ethical maturity levels. Within the scope of the survey, the participants were asked the question, 'As a cybersecurity of 1-10, the same expert panel conducted, what are the following ethical values for you?'. The survey form was designed to allow participants to rate each ethical value on a scale of 1 to 10. With this structure, participants could assign the same score to more than one ethical value; thus, they could make a prioritization that was more flexible, realistic, and in line with personal values. As a result of the application, a total of 37 valid responses were obtained and included in the analysis process. Ethical codes published by ACM, IEEE, (ISC)<sup>2</sup>, ISACA, NIST, and UK Cyber Security Council were used to define ethical values. This approach enabled an evaluation process based on individual perceptions and professional and organizational ethical norms. The data obtained were analyzed based on the participants' scores, revealing the relative importance levels of the ethical values. These findings provide a strong basis for modelling the level of ethical maturity.

Table 5. Software tools and computational environment used in the study

Component	Tool / Library	Version	Purpose in workflow
Programming language	Python	3.13.5	Scripting for data processing and AHP computations (Eqs. 4 - 7)
Data analysis	Pandas	$\geq 2.2$	Reading/cleaning survey data; column-normalization; row-average weights
Numerical computing	NumPy	$\geq 1.26$	Vector/matrix operations $A_w$ , $\lambda_{max}$ estimation. Used in Eq. (6) and CI/CR calculations (Eqs. 7 and 8).
Excel I/O	Openpyxl	$\geq 3.1$	Exporting and importing matrices and results to .xlsx produced the tables reported in the Results section.
Spreadsheet	Microsoft Excel (Microsoft 365, desktop)	16	Manual matrix entry; quick checks; figure/table formatting. Column totals, quick sanity checks, and figure exports.

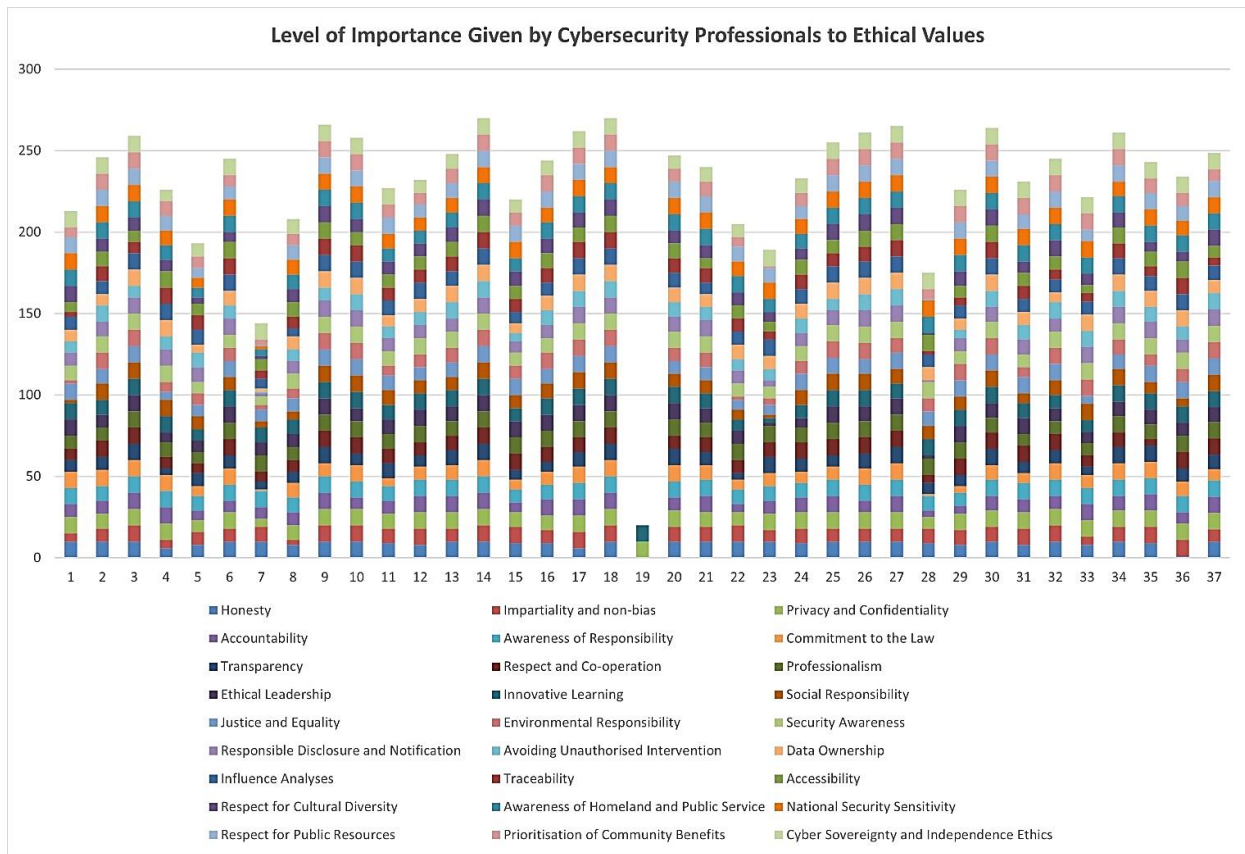


Figure 1. Levels of Importance Given by Cybersecurity Professionals to Ethical Values

The participants were cybersecurity professionals with 5 to 10 years of experience in the field. To preserve anonymity and reduce the burden of responding, information about sector and job role was not collected. In addition to providing 1-10 ratings, the same expert panel completed an AHP pairwise comparison exercise for the ethical criteria. To enhance transparency and reproducibility, the software environment used in data handling and AHP calculations is summarized in Table 5.

### 3.2. AHP Application Process

The AHP is a systematic and quantitative method for solving multi-criteria decision-making problems. This approach, which was first introduced by Myers and Alpert (1968) within the scope of multidimensional preference modelling, was transformed into a formal model by Thomas L. Saaty in 1977 and turned into a framework applicable in decision-making processes. AHP allows decision-makers to analyze complex problems by simplifying them in a hierarchical structure. This method establishes priority relationships between decision points and the factors affecting them through pairwise comparisons. Each decision factor is evaluated against the others on a scale of 1 to 9, and relative importance levels are calculated based on these evaluations. The resulting  $n \times n$  square matrix contains a quantitative expression of the relative importance of the relevant criteria. The diagonal elements of the matrix take the value 1, assuming that each criterion is of equal significance to itself. This structure turns into a symmetric comparison matrix as shown in Equation (1) [13].

$$\begin{bmatrix}
 a_{11} & a_{12} & \dots & a_{1n} \\
 a_{21} & a_{22} & \dots & a_{2n} \\
 \vdots & \vdots & \ddots & \vdots \\
 a_{1n} & a_{2n} & \dots & a_{nn}
 \end{bmatrix} \tag{1}$$

The comparison matrix makes comparisons for all upper triangular elements above the value 1. Naturally, for the components in the lower triangle of the matrix, it is sufficient to use the formula in Equation (2).

$$a_{ij} = \frac{1}{a_{ji}} \tag{2}$$

To explain through the given example, when the value at the intersection of the first row and the third column in the comparison matrix ( $i = 1, j = 3$ ) is determined as 3, the component in the third row and the first column ( $i = 3, j = 1$ ), which is symmetrical to this evaluation, will automatically be  $1/3$ . This is based on the pairwise comparison logic used in the AHP

method. The importance levels of AHP are expressed in numerical scales reflecting the extent to which the decision maker prefers one element over another. The values of this scaling system are presented in detail in Table 6.

Table 6. AHP Importance Scale

Importance Value	Description
1	When both factors are equally important
3	When the first factor is slightly more important than the second factor
5	When the first factor is strongly more important than the second factor
7	When the first factor has a considerably more dominant importance than the second factor
9	When the first factor is superior to the second factor
2, 4, 6, 8	Intermediate values reflect intermediate preferences between two basic levels of importance.

In the AHP method, decision-makers are expected to compare two criteria and indicate to what extent one is more important than the other. These comparisons are expressed numerically within a particular scale. Single numbers such as 1, 3, 5, 7, and 9 form the basis of the scale, while the values 2, 4, 6, and 8 are used to indicate intermediate preferences between these basic levels. For example, a value of 1 indicates that two criteria are equally important, while a value of 9 represents the absolute superiority of one criterion over the other. This systematic structure ensures that subjective assessments become consistent and comparable. The values obtained from the comparisons are normalized by dividing each value by the relevant column total, and the weight coefficients of the criteria are calculated by averaging the values in each row. As a result of this process, a consistent and measurable prioritization structure is obtained to guide the decision-making process. Equation (3) shows the calculation process of the normalized pairwise comparison matrix.

$$B_i = \begin{bmatrix} b_{11} \\ b_{21} \\ \vdots \\ b_{n1} \end{bmatrix} \tag{3}$$

Pairwise comparisons within the scope of the AHP method allow subjective evaluation criteria to be expressed systematically and numerically. This structure enhances the reliability of the evaluation process by making the individual judgments of decision-makers controllable through consistency checks. The performance criteria for selecting a patch management application in this study were structured using the AHP method. The evaluation process was conducted with the participation of numerous professionals specializing in information technology, and weighted averages were calculated based on the opinions gathered. Thus, the relative importance levels of the criteria were determined more accurately. Equation (4) illustrates the calculation method for the normalized pairwise comparison matrix, a key component of this process.

$$b_{ij} = \frac{a_{ij}}{\sum_{i=1}^n a_{ij}} \tag{4}$$

After obtaining the column-normalized matrix  $B = [b_{ij}]$ , the priority vector is derived by the row-average method. For each criterion  $i$ :

$$w_i = \frac{1}{n} \sum_{j=1}^n b_{ij} \tag{5}$$

Let  $w = [w_1, \dots, w_n]^T$  denote the weight vector and  $A = [a_{ij}]$  the original (non-normalised) pairwise matrix. The maximum eigenvalue  $\lambda_{max}$ , which is required for consistency analysis, is estimated as follows:

$$\lambda_{max} = \frac{1}{n} \sum_{i=1}^n \frac{(Aw)_i}{w_i} \tag{6}$$

Subsequently, the Consistency Index (CI) and Consistency Ratio (CR) are computed using Equations (7) and (8):

$$CI = \frac{\lambda_{max} - n}{n - 1} \tag{7}$$

$$CR = \frac{CI}{RI_n} \tag{8}$$

Here  $RI_n$  represents Saaty’s Random Index for a matrix of order  $n$ .  $n = 27, RI_{27} = 1.6631$  [38]. According to standard AHP practices, a Consistency Ratio of less than,  $CR < 0.10$  indicates that the judgement matrix demonstrates acceptable consistency [13]. RI values shown in Figure 2.

Order	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RI	0	0	0.52	0.89	1.12	1.26	1.36	1.41	1.46	1.49	1.52	1.54	1.56	1.58	1.59
Order	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
RI	1.5943	1.6064	1.6133	1.6207	1.6292	1.6385	1.6403	1.6462	1.6497	1.6556	1.6587	1.6631	1.667	1.6693	1.6724

Figure 2. RI Values [38]

### 3.3. Proposed Cybersecurity Ethical Maturity Model

This study developed a new ethical maturity model based on a five-stage process: (1) Awareness, (2) Initiation, (3) Structured, (4) Integrated, and (5) Excellence. This proposed five-stage structure draws inspiration from organizational maturity models in the literature, especially the Community Cyber Security Maturity Model (CCSMM). The CCSMM addresses not only technical capacity but also multidimensional factors, such as ethical awareness, leadership, communication, and social awareness. Its structure begins with awareness and evolves into a dynamic security culture through institutionalization over time. The developed model is rooted in this multi-layered structure of CCSMM and emphasizes the integration of ethical values into institutional processes in a hierarchical manner. Therefore, a measurable development path is outlined, where ethical principles are defined in terms of individual attitudes and strategic organizational competencies. A specific set of ethical values characterizes each level. For instance, the Awareness stage includes values that ‘need to be noticed’ but are not yet reflected in corporate practice, such as transparency, traceability, and respect for cultural diversity. The Excellence stage fully institutionalizes strategic and critical values, such as privacy and confidentiality, accountability, cyber sovereignty, and independent ethics. Figure 3 illustrates the comprehensive architecture of the model, with the ethical value sets corresponding to each level presented in a mind map format.

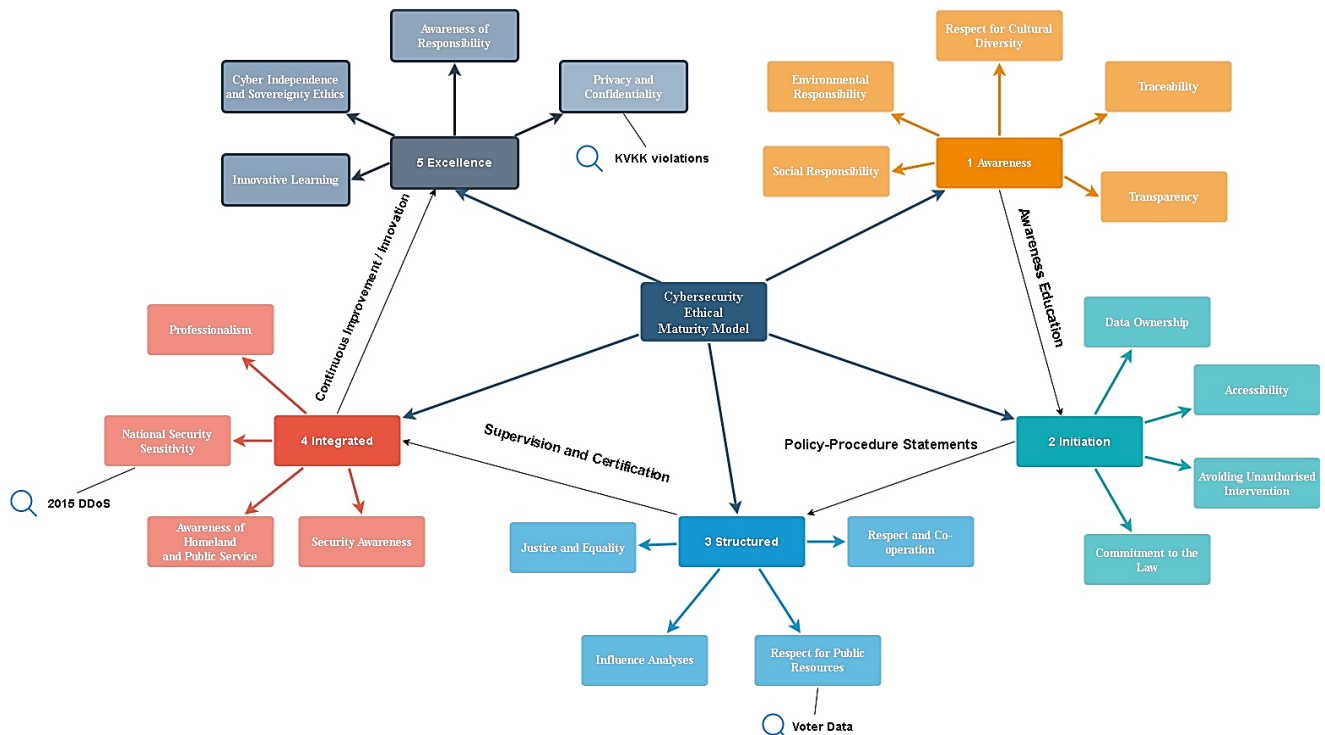


Figure 3. Mind map of the Cybersecurity Ethical Maturity Model

Figure 3 illustrates the model's overall structure along with the ethical value sets for each level, depicted as a mind map. When examined, the Awareness level is associated with low critical values based on transparency. In contrast, the Excellence stage is characterized by high-critical values that focus on privacy, confidentiality, and awareness of responsibility. The Initial, Structured, and Integrated stages serve as intermediate transition points between these levels, supported by policy and procedure statements, supervision and certification mechanisms, and continuous improvement and innovation strategies,

respectively. This structure provides a practical framework for assessing an organization’s current ethical capacity and identifying steps to reach the next level. For an interpretation of the model in conjunction with the AHP results, see Chapter 4.

#### 4. Findings and Discussion

##### 4.1. Findings

This study used the statistical average method and the AHP to evaluate the importance of ethical values in cybersecurity. In the first step, participant scores for each ethical value were added up, divided by the total number of participants (n = 37), and the average importance of each value was calculated. This approach showed the general trend of how professionals prioritize ethical values. In the second step, a pairwise comparison matrix was created using the AHP method based on expert opinions, and the relative weight coefficients of each ethical value were determined through this matrix. The weight vectors, obtained by normalizing the comparison matrix, were scaled to express the proportional importance of each ethical value as a percentage of 100%. Combining these two methods obtained participant-based overall trends and analytical weight values from expert evaluations. Detailed results are shown in Tables 7, 8, and 9.

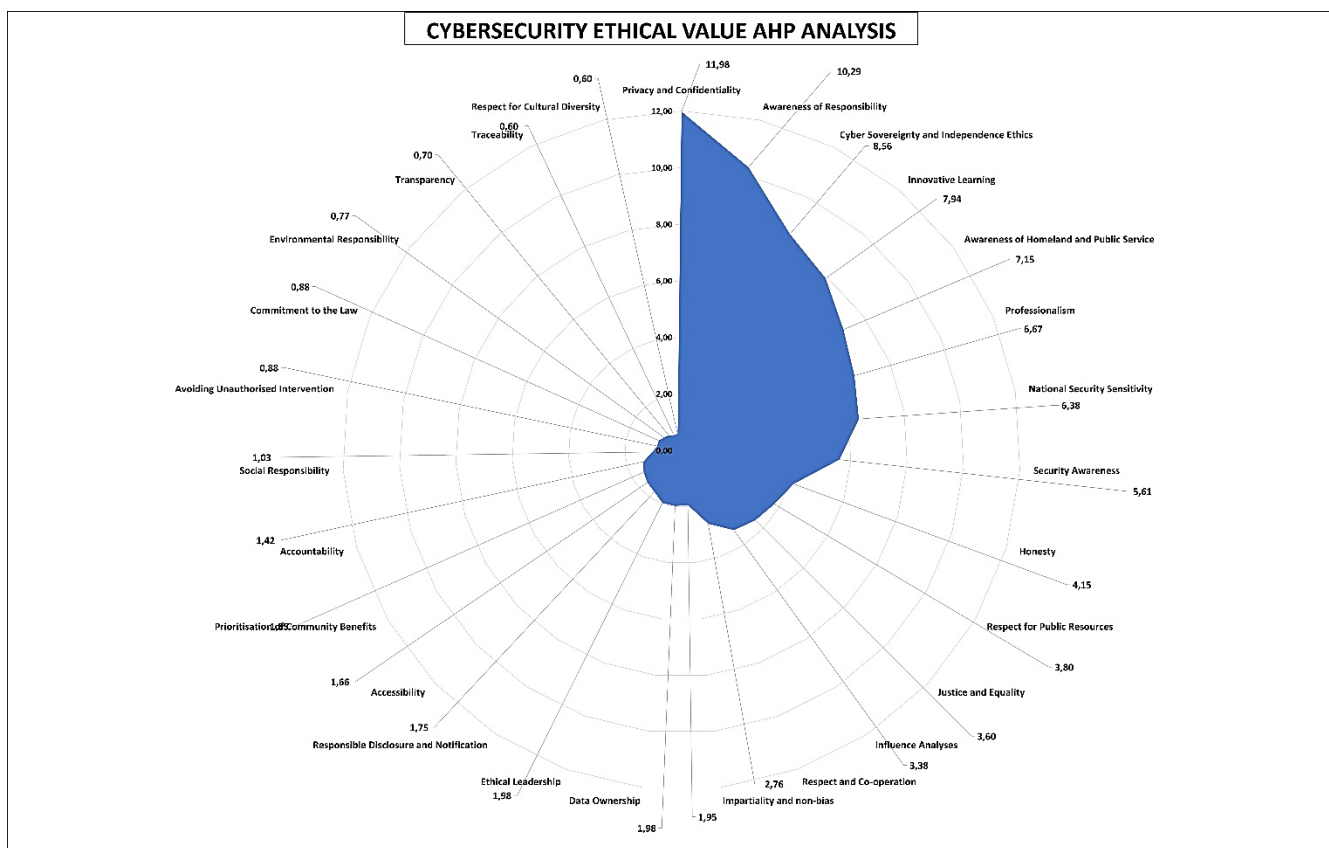


Figure 4. Cybersecurity Ethical Value AHP Analysis Radar Graphic

Tables 7 and 8 reflect the details of the calculations related to the AHP process conducted in this study. In Table 7, the relative weight coefficients of each ethical value are calculated together with the pairwise comparison matrix created based on expert opinions and the normalized values obtained from this matrix. The comparative importance levels of ethical values relative to one another are presented in the upper part of the matrix. The total contributions and rankings of these values in their normalized form are provided in the lower part. Thus, the relative importance of ethical values was analyzed systematically. Tables 8 and 9 present the normalization and ranking of these weights in percentage terms. This representation enables decision-makers to compare and prioritize among ethical values. According to the AHP analysis, Confidentiality and Privacy stand out as the most important ethical values, with 11.98%, Awareness of Responsibility with 10.29% and Cyber Sovereignty and Independence Ethics with 8.56%. This ranking reveals the ethical prioritization of experts working in the field of cybersecurity.

Table 7. Ethical Values Pairwise Comparison Matrix Based on the AHP Method

Ethical Value	Privacy and Confidentiality	Awareness of Responsibility	Cyber Sovereignty and Independence Ethics	Innovative Learning	Awareness of Homeland and Public	Professionalism	National Security Sensitivity	Security Awareness	Honesty	Respect for Public Resources	Justice and Equality	Influence Analyses	Respect and Co-operation	Impartiality and non-bias	Data Ownership	Ethical Leadership	Responsible Disclosure and Notification	Accessibility	Prioritisation of Community Benefits	Accountability	Social Responsibility	Avoiding Unauthorised Intervention	Commitment to the Law	Environmental Responsibility	Transparency	Traceability	Respect for Cultural Diversity
Privacy and Confidentiality	1	2	2	3	3	3	3	3	4	5	5	5	5	6	6	6	7	7	7	7	8	8	8	9	9	9	9
Awareness of Responsibility	1/2	1	2	2	2	3	3	3	4	4	4	4	5	6	6	6	6	6	6	7	8	8	8	8	9	9	9
Cyber Sovereignty and Independence Ethics	1/2	1/2	1	2	2	2	2	2	3	4	4	4	4	5	5	5	6	6	6	6	7	7	7	8	8	8	8
Innovative Learning	1/3	1/2	1/2	1	2	2	2	2	3	4	4	4	4	5	5	5	5	6	6	6	7	7	7	7	8	8	8
Awareness of Homeland and Public Service	1/3	1/2	1/2	1/2	1	2	2	2	3	3	3	3	4	5	5	5	5	5	5	6	7	7	7	7	7	8	8
Professionalism	1/3	1/3	1/2	1/2	1/2	1	2	2	3	3	3	3	4	5	5	5	5	5	5	5	6	7	7	7	7	8	8
National Security Sensitivity	1/3	1/3	1/2	1/2	1/2	1/2	1	2	3	3	3	3	4	5	5	5	5	5	5	5	6	7	7	7	7	8	8
Security Awareness	1/3	1/3	1/2	1/2	1/2	1/2	1/2	1	2	3	3	3	3	4	4	4	5	5	5	5	6	6	6	7	7	7	7
Honesty	1/4	1/4	1/3	1/3	1/3	1/3	1/3	1/2	1	2	2	2	2	3	3	3	4	4	4	4	5	5	5	6	6	6	6
Respect for Public Resources	1/5	1/4	1/4	1/4	1/3	1/3	1/3	1/3	1/2	1	2	2	2	3	3	3	3	4	4	4	5	5	5	5	6	6	6
Justice and Equality	1/5	1/4	1/4	1/4	1/3	1/3	1/3	1/3	1/2	1/2	1	2	2	3	3	3	3	3	4	4	5	5	5	5	6	6	6
Influence Analyses	1/5	1/4	1/4	1/4	1/3	1/3	1/3	1/3	1/2	1/2	1/2	1	2	3	3	3	3	3	3	4	5	5	5	5	5	6	6
Respect and Co-operation	1/5	1/5	1/4	1/4	1/4	1/4	1/4	1/3	1/2	1/2	1/2	1/2	1	2	2	2	3	3	3	3	4	4	4	4	5	5	5
Impartiality and non-bias	1/6	1/6	1/5	1/5	1/5	1/5	1/5	1/4	1/3	1/3	1/3	1/3	1/2	1	1	1	2	2	2	2	3	3	3	4	4	4	4
Data Ownership	1/6	1/6	1/5	1/5	1/5	1/5	1/5	1/4	1/3	1/3	1/3	1/3	1/2	1	1	1	2	2	2	2	3	3	3	4	4	4	4
Ethical Leadership	1/6	1/6	1/5	1/5	1/5	1/5	1/5	1/4	1/3	1/3	1/3	1/3	1/2	1	1	1	2	2	2	2	3	3	3	4	4	4	4

**Table 7(Continued)**

Ethical Value	Privacy and Confidentiality	Awareness of Responsibility	Cyber Sovereignty and Independence Ethics	Innovative Learning	Awareness of Homeland and Public Service	Professionalism	National Security Sensitivity	Security Awareness	Honesty	Respect for Public Resources	Justice and Equality	Influence Analyses	Respect and Co-operation	Impartiality and non-bias	Data Ownership	Ethical Leadership	Responsible Disclosure and Notification	Accessibility	Prioritisation of Community Benefits	Accountability	Social Responsibility	Avoiding Unauthorised Intervention	Commitment to the Law	Environmental Responsibility	Transparency	Traceability	Respect for Cultural Diversity
Responsible Disclosure and Notification	1/7	1/6	1/6	1/5	1/5	1/5	1/5	1/5	1/4	1/3	1/3	1/3	1/3	1/2	1/2	1/2	1	2	2	2	3	3	3	3	4	4	4
Accessibility	1/7	1/6	1/6	1/6	1/5	1/5	1/5	1/5	1/4	1/4	1/3	1/3	1/3	1/2	1/2	1/2	1/2	1	2	2	3	3	3	3	4	4	4
Prioritisation of Community Benefits	1/7	1/6	1/6	1/6	1/5	1/5	1/5	1/5	1/4	1/4	1/4	1/3	1/3	1/2	1/2	1/2	1/2	1/2	1	2	3	3	3	3	3	4	4
Accountability	1/7	1/7	1/6	1/6	1/6	1/5	1/5	1/5	1/4	1/4	1/4	1/4	1/3	1/2	1/2	1/2	1/2	1/2	1/2	1	2	3	3	3	3	4	4
Social Responsibility	1/8	1/8	1/7	1/7	1/7	1/6	1/6	1/6	1/5	1/5	1/5	1/5	1/4	1/3	1/3	1/3	1/3	1/3	1/3	1/2	1	2	2	2	2	3	3
Avoiding Unauthorised Intervention	1/8	1/8	1/7	1/7	1/7	1/7	1/7	1/6	1/5	1/5	1/5	1/5	1/4	1/3	1/3	1/3	1/3	1/3	1/3	1/2	1	2	2	2	2	2	2
Commitment to the Law	1/8	1/8	1/7	1/7	1/7	1/7	1/7	1/6	1/5	1/5	1/5	1/5	1/4	1/3	1/3	1/3	1/3	1/3	1/3	1/2	1	1	2	2	2	2	2
Environmental Responsibility	1/9	1/8	1/8	1/7	1/7	1/7	1/7	1/7	1/6	1/5	1/5	1/5	1/4	1/3	1/4	1/4	1/3	1/7	1/3	1/3	1/2	1/2	1/2	1	2	2	2
Transparency	1/9	1/9	1/8	1/8	1/7	1/7	1/7	1/7	1/6	1/6	1/6	1/5	1/5	1/4	1/4	1/4	1/4	1/4	1/3	1/3	1/2	1/2	1/2	1/2	1	2	2
Traceability	1/9	1/9	1/8	1/8	1/8	1/8	1/8	1/7	1/6	1/6	1/6	1/6	1/5	1/4	1/4	1/4	1/4	1/4	1/4	1/4	1/3	1/2	1/2	1/2	1/2	1	1
Respect for Cultural Diversity	1/9	1/9	1/8	1/8	1/8	1/8	1/8	1/7	1/6	1/6	1/6	1/6	1/5	1/4	1/4	1/4	1/4	1/4	1/4	1/4	1/3	1/2	1/2	1/2	1/2	1	1
Total	6.61	8.68	11.03	13.58	15.41	17.97	19.47	21.45	31.27	36.88	38.47	40.08	46.43	62.08	62.00	62.00	70.58	73.89	76.67	81.33	102.67	108.00	108.00	116.50	126.00	135.00	135.00

Table 8. AHP Weight Coefficients of Ethical Values

Ethical Value	Privacy and Confidentiality	Awareness of Responsibility	Cyber Sovereignty and Independence Ethics	Innovative Learning	Awareness of Homeland and Public	Professionalism	National Security Sensitivity	Security Awareness	Honesty	Respect for Public Resources	Justice and Equality	Influence Analyses	Respect and Co-operation	Impartiality and non-bias	Data Ownership	Ethical Leadership	Responsible Disclosure and Notification	Accessibility	Prioritisation of Community Benefits	Accountability	Social Responsibility	Avoiding Unauthorised Intervention	Commitment to the Law	Environmental Responsibility	Transparency	Traceability	Respect for Cultural Diversity
Privacy and Confidentiality	0.15	0.23	0.18	0.22	0.19	0.17	0.15	0.14	0.13	0.14	0.13	0.12	0.11	0.10	0.10	0.10	0.10	0.09	0.09	0.09	0.08	0.07	0.07	0.08	0.07	0.07	0.07
Awareness of Responsibility	0.08	0.12	0.18	0.15	0.13	0.17	0.15	0.14	0.13	0.11	0.10	0.10	0.11	0.10	0.10	0.10	0.09	0.08	0.08	0.09	0.08	0.07	0.07	0.07	0.07	0.07	0.07
Cyber Sovereignty and Independence Ethics	0.08	0.06	0.09	0.15	0.13	0.11	0.10	0.09	0.10	0.11	0.10	0.10	0.09	0.08	0.08	0.08	0.09	0.08	0.08	0.07	0.07	0.06	0.06	0.07	0.06	0.06	0.06
Innovative Learning	0.05	0.06	0.05	0.07	0.13	0.11	0.10	0.09	0.10	0.11	0.10	0.10	0.09	0.08	0.08	0.08	0.07	0.08	0.08	0.07	0.07	0.06	0.06	0.06	0.06	0.06	0.06
Awareness of Homeland and Public Service	0.05	0.06	0.05	0.04	0.06	0.11	0.10	0.09	0.10	0.08	0.08	0.07	0.09	0.08	0.08	0.08	0.07	0.07	0.07	0.07	0.07	0.06	0.06	0.06	0.06	0.06	0.06
Professionalism	0.05	0.04	0.05	0.04	0.03	0.06	0.10	0.09	0.10	0.08	0.08	0.07	0.09	0.08	0.08	0.08	0.07	0.07	0.07	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06
National Security Sensitivity	0.05	0.04	0.05	0.04	0.03	0.03	0.05	0.09	0.10	0.08	0.08	0.07	0.09	0.08	0.08	0.08	0.07	0.07	0.07	0.06	0.06	0.06	0.06	0.06	0.06	0.06	0.06
Security Awareness	0.05	0.04	0.05	0.04	0.03	0.03	0.03	0.05	0.06	0.08	0.08	0.07	0.06	0.06	0.06	0.06	0.07	0.07	0.07	0.06	0.06	0.06	0.06	0.06	0.06	0.05	0.05
Honesty	0.04	0.03	0.03	0.02	0.02	0.02	0.02	0.02	0.03	0.05	0.05	0.05	0.04	0.05	0.05	0.05	0.06	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.04	0.04
Respect for Public Resources	0.03	0.03	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.03	0.05	0.05	0.04	0.05	0.05	0.05	0.04	0.05	0.05	0.05	0.05	0.05	0.05	0.04	0.05	0.04	0.04
Justice and Equality	0.03	0.03	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.01	0.03	0.05	0.04	0.05	0.05	0.05	0.04	0.04	0.05	0.05	0.05	0.05	0.05	0.04	0.05	0.04	0.04
Influence Analyses	0.03	0.03	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.01	0.01	0.02	0.04	0.05	0.05	0.05	0.04	0.04	0.04	0.05	0.05	0.05	0.05	0.04	0.04	0.04	0.04
Respect and Co-operation	0.03	0.02	0.02	0.02	0.02	0.01	0.01	0.02	0.02	0.01	0.01	0.01	0.02	0.03	0.03	0.03	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.03	0.04	0.04	0.04
Impartiality and non-bias	0.03	0.02	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.02	0.02	0.02	0.03	0.03	0.03	0.02	0.03	0.03	0.03	0.03	0.03	0.03	0.03
Data Ownership	0.03	0.02	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.02	0.02	0.02	0.03	0.03	0.03	0.02	0.03	0.03	0.03	0.03	0.03	0.03	0.03
Ethical Leadership	0.03	0.02	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.02	0.02	0.02	0.03	0.03	0.03	0.02	0.03	0.03	0.03	0.03	0.03	0.03	0.03

**Table 8(Continued)**

<b>Ethical Value</b>	<b>Privacy and Confidentiality</b>	<b>Awareness of Responsibility</b>	<b>Cyber Sovereignty and Independence Ethics</b>	<b>Innovative Learning</b>	<b>Awareness of Homeland and Public Service</b>	<b>Professionalism</b>	<b>National Security Sensitivity</b>	<b>Security Awareness</b>	<b>Honesty</b>	<b>Respect for Public Resources</b>	<b>Justice and Equality</b>	<b>Influence Analyses</b>	<b>Respect and Co-operation</b>	<b>Impartiality and non-bias</b>	<b>Data Ownership</b>	<b>Ethical Leadership</b>	<b>Responsible Disclosure and Notification</b>	<b>Accessibility</b>	<b>Prioritisation of Community Benefits</b>	<b>Accountability</b>	<b>Social Responsibility</b>	<b>Avoiding Unauthorised Intervention</b>	<b>Commitment to the Law</b>	<b>Environmental Responsibility</b>	<b>Transparency</b>	<b>Traceability</b>	<b>Respect for Cultural Diversity</b>	
Responsible Disclosure and Notification	0.02	0.02	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.03	0.03	0.02	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
Accessibility	0.02	0.02	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.03	0.02	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
Prioritisation of Community Benefits	0.02	0.02	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.02	0.03	0.03	0.03	0.03	0.02	0.03	0.03	0.03
Accountability	0.02	0.02	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.02	0.03	0.03	0.03	0.02	0.03	0.03	0.03
Social Responsibility	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.00	0.01	0.01	0.01	0.01	0.00	0.00	0.00	0.01	0.01	0.02	0.02	0.02	0.02	0.02	0.02	0.02
Avoiding Unauthorised Intervention	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.00	0.01	0.01	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.01	0.01	0.02	0.02	0.01	0.01	0.01
Commitment to the Law	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.00	0.01	0.01	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.01	0.01	0.02	0.02	0.01	0.01	0.01
Environmental Responsibility	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.00	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.02	0.01	0.01	0.01
Transparency	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.01	0.01	0.01
Traceability	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.01	0.01
Respect for Cultural Diversity	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.01	0.01
Total	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

Table 9. Normalized Percentages and Importance Weights of Ethical Values

Ethical Value	Normalized Total	Weight	Normalized Total Percentage Value and Order of Importance (%)
Privacy and Confidentiality	3.24	0.12	11.98
Awareness of Responsibility	2.78	0.10	10.29
Cyber Sovereignty and Independence Ethics	2.31	0.09	8.56
Innovative Learning	2.14	0.08	7.94
Awareness of Homeland and Public Service	1.93	0.07	7.15
Professionalism	1.80	0.07	6.67
National Security Sensitivity	1.72	0.06	6.38
Security Awareness	1.51	0.06	5.61
Honesty	1.12	0.04	4.15
Respect for Public Resources	1.02	0.04	3.80
Justice and Equality	0.97	0.04	3.60
Influence Analyses	0.91	0.03	3.38
Respect and Co-operation	0.75	0.03	2.76
Impartiality and non-bias	0.53	0.02	1.95
Data Ownership	0.54	0.02	1.98
Ethical Leadership	0.54	0.02	1.98
Responsible Disclosure and Notification	0.47	0.02	1.75
Accessibility	0.45	0.02	1.66
Prioritisation of Community Benefits	0.42	0.02	1.55
Accountability	0.38	0.01	1.42
Social Responsibility	0.28	0.01	1.03
Avoiding Unauthorised Intervention	0.24	0.01	0.88
Commitment to the Law	0.24	0.01	0.88
Environmental Responsibility	0.21	0.01	0.77
Transparency	0.19	0.01	0.70
Traceability	0.16	0.01	0.60
Respect for Cultural Diversity	0.16	0.01	0.60
Total	27.00	1.00	100.00

Radar Graph in Figure 4, designed as a visual summary of these findings, clearly illustrates the distribution of ethical values based on their AHP weights. In the graph, it is apparent that Confidentiality and Privacy, the ethical values with the highest importance, stand out prominently; other values are positioned on the graph according to their relative magnitudes. The fact that especially low-scoring values, such as Respect for Cultural Diversity, Traceability, and Transparency, are located near the center of the radar chart emphasizes the need for increased awareness and improvement in these areas. This graph is a crucial tool for decision-makers and institutions to visually compare ethical values and guide policy development processes.

The Consistency Ratio (CR) obtained from the pairwise comparison matrix was calculated as 4.88%, which is well below the generally accepted threshold of 10%. This result indicates that the expert judgments in the pairwise comparisons are consistent and reliable. Therefore, the AHP-derived prioritization of ethical values in this study can be considered both valid and statistically coherent. The consistency analysis results of the AHP matrix are shown in Table 10.

#### 4.2. Discussion

The results reveal a clear hierarchy in how cybersecurity professionals perceive ethical values. Privacy and Confidentiality were identified as the most significant ethical dimensions, 11.98%, followed by Awareness of Responsibility, 10.29% and

Cyber Sovereignty and Independence Ethics, 8.56%. These findings indicate that experts place strong emphasis on data security, personal privacy, and national digital sovereignty. Considering the rising cyber threats and the growing concerns surrounding digital surveillance, these priorities are consistent with the dual focus on individual ethical responsibility and national cybersecurity resilience.

Table 10. Consistency Analysis Results of the AHP Matrix

n	RI	$\lambda_{max}$	CI	CR	CR (%)
27	1.6631	29.11	0.08	0.05	4.88

Conversely, the relatively low importance attributed to Transparency, Traceability, Environmental Responsibility, and Respect for Cultural Diversity suggests that ethical education in cybersecurity should not be limited to technical and security-oriented principles. Instead, it should also integrate social, environmental, and cultural dimensions to foster a more holistic understanding of ethical responsibility in digital environments.

The integration of both statistical averaging and AHP-based analysis in this study allowed the development of an objective, data-driven ethical prioritization framework based on expert opinions. This structure provides strategic guidance for organizations aiming to design ethical education programs and develop policy frameworks grounded in empirical evidence. Moreover, targeted awareness initiatives focusing on lower-weighted ethical values could play a vital role in cultivating a more comprehensive cybersecurity culture.

When compared with Figure 3, representing the five-stage CEMM introduced in Section 3.3, the findings demonstrate strong internal consistency. Values such as Transparency, Traceability, and Respect for Cultural Diversity, located within the Awareness stage of the model, correspond to the lower range of Table 7 (0.4 - 0.5%), indicating that these values are not yet fully embedded within organizational ethics. In contrast, Privacy and Confidentiality 11.98%, Awareness of Responsibility 10.29%, and Cyber Sovereignty and Independence Ethics 8.56%, core elements of the Excellence stage, form the outer perimeter of the radar chart, aligning with expectations at the highest maturity level. The pairwise comparisons and resulting weights were directly mapped to the corresponding ethical maturity levels defined in the CEMM model, thereby linking each ethical criterion to its developmental stage. This operational mapping clarifies how value clusters such as transparency, traceability, and cultural diversity are positioned within the Awareness stage, while high-weighted values such as privacy, confidentiality, and responsibility awareness correspond to the Excellence stage, illustrating the hierarchical transition between ethical awareness and institutionalization.

The clustering of values such as Commitment to the Law (0.63%), Justice and Equality (3.55%), and Innovative Learning (7.73%) in intermediate positions, corresponding to the Initial, Structured, and Integrated stages, suggests that organizations tend to prioritize foundational compliance and fairness-related concerns before advancing toward innovation and continuous improvement strategies. Therefore, the weight distributions derived from the AHP analysis empirically reinforce the progression logic of the maturity model and enhance its confirmatory validity.

Future research can build upon the findings of this study in a number of ways. Firstly, including professionals from diverse sectors, such as public administration, finance, health, and critical infrastructure, in the participant base would enhance the representativeness and generalizability of the proposed CEMM. Secondly, alternative multi-criteria decision-making techniques could be useful in validating and comparing the robustness of the obtained prioritization results, such as the Analytic Network Process (ANP), Best-Worst Method (BWM), or Fuzzy Analytic Hierarchy Process (FAHP). Thirdly, incorporating real-world incident data and key performance indicators, such as breach frequency, response efficiency, and public trust metrics, into longitudinal studies would provide empirical evidence with which to assess the model's predictive capacity and practical utility.

Furthermore, future research should examine the integration of the ethical maturity assessment framework into existing national and organizational audit mechanisms, such as ISO/IEC 27001 and the Information and Communication Security Guide (BİGR), with the aim of establishing a unified structure for ethics-based governance. Cross-cultural comparative analyses between Türkiye and other countries could also help to clarify the influence of socio-cultural contexts on ethical awareness and maturity in cybersecurity practices. These multidisciplinary, empirical extensions would strengthen the theoretical basis of the proposed framework and make its policies more relevant.

## 5. Conclusion

This study examines ethical maturity in the cybersecurity profession in a measurable and phased manner, utilizing survey data and the AHP approach in conjunction. Responses from 37 experts across Türkiye were used to quantitatively determine the priority weights of 27 ethical values aligned with internationally recognized codes (ACM, IEEE, (ISC)<sup>2</sup>, ISACA, NIST, and UK CSC). The resulting pairwise comparison matrix produced a consistent solution (CR = 4.88%). The top three priorities were privacy and confidentiality (11.98%), responsibility awareness (10.29%), and Cyber Sovereignty and Independence Ethics (8.56%). Conversely, transparency (0.70%), traceability (0.60%), and respect for cultural diversity (0.60%) received the lowest weights, indicating that these values were not sufficiently reflected in corporate practices. These weights were then matched with the five-level CEMM and tested for internal consistency. The low-weighted values being

placed at the Awareness level in the model and the high-weighted values centered on privacy and responsibility being placed at the Excellence level confirm that empirical data validate the maturity logic. Values in the middle tiers, which focus on regulatory compliance, auditing/certification, and improvement dimensions, define the thresholds on which organizations should focus during the establishment, structured, and integrated transitions.

Seven current events, selected from the Türkiye context, were analyzed using the model. These events were: the large-scale DDoS attacks in 2015; the e-commerce data breach in 2018; the targeting of Ministry of Health data during the 2019–2020 period of the pandemic; the mobile banking and SMS phishing attempts in 2021; the GSM operator customer data leak in 2022; the claim in 2023 that ‘85 million e-Government data were leaked’; and the TürkNet customer data incident in 2025. Incidents that violate the principle of privacy and confidentiality, which carries the highest weight, are associated with the most confidence-eroding and systemically impactful outcomes. Examples include the TürkNet and e-Government cases, as well as the GSM and e-commerce cases. Delays or ambiguities in crisis communication have accompanied weaknesses in the principles of transparency and accountability. The insufficient internalization of responsibility awareness in practice has also emerged as a recurring finding. These findings validate the model's diagnostic power, showing that high-impact failures correspond to gaps in high-priority ethical values and that weak crisis performance corresponds to deficiencies in operationally critical but low-priority values.

In conclusion, this study offers three main contributions to cybersecurity professionals, decision-makers, and training designers: an AHP-based priority map quantifying ethical values, an ethical maturity model that embodies the organizational development path at five levels, and an action plan for policy, supervision, and training interventions through model and case matching. It is considered critical for organizations to invest in relatively low-scoring areas such as transparency and cultural sensitivity, as well as privacy and confidentiality, and an awareness of responsibility, and to update the maturity model with a continuous improvement cycle to build a sustainable cyber ecosystem with high public trust.

## Appendix A. Survey Form Used in the Study

**Title:** Cybersecurity Professionals' Views on Ethical Values

### Instructions for Participants:

As a cybersecurity professional, please rate the importance level of each ethical value listed below on a scale from 1 to 10, where 1 = Least Important and 10 = Most Important. You may assign the same score to multiple values according to your personal judgment. No personal or identifiable information was collected, and participation was entirely voluntary and anonymous.

Ethical Value	Score (1-10)
Honesty	<input type="checkbox"/> _____
Accountability	<input type="checkbox"/> _____
Transparency	<input type="checkbox"/> _____
Ethical Leadership	<input type="checkbox"/> _____
Justice and Equality	<input type="checkbox"/> _____
Responsible Disclosure and Notification	<input type="checkbox"/> _____
Influence Analyses	<input type="checkbox"/> _____
Respect for Cultural Diversity	<input type="checkbox"/> _____
Respect for Public Resources	<input type="checkbox"/> _____
Impartiality and non-bias	<input type="checkbox"/> _____
Awareness of Responsibility	<input type="checkbox"/> _____
Respect and Co-operation	<input type="checkbox"/> _____
Innovative Learning	<input type="checkbox"/> _____
Environmental Responsibility	<input type="checkbox"/> _____
Avoiding Unauthorised Intervention	<input type="checkbox"/> _____
Traceability	<input type="checkbox"/> _____
Awareness of Homeland and Public Service	<input type="checkbox"/> _____
Prioritisation of Community Benefits	<input type="checkbox"/> _____
Privacy and Confidentiality	<input type="checkbox"/> _____
Commitment to the law	<input type="checkbox"/> _____
Professionalism	<input type="checkbox"/> _____
Social Responsibility	<input type="checkbox"/> _____
Security Awareness	<input type="checkbox"/> _____
Data Ownership	<input type="checkbox"/> _____
Accessibility	<input type="checkbox"/> _____
National Security and Sensitivity	<input type="checkbox"/> _____
Cyber Sovereignty and Independence Ethics	<input type="checkbox"/> _____

## References

- [1] A. Benlahcene, R. B. Zainuddin, N. Syakiran, and A. B. Ismail, "A narrative review of ethics theories: teleological & deontological ethics," *J. Humanities Soc. Sci. (IOSR-JHSS)*, vol. 23, no. 1, pp. 31–32, 2018.
- [2] "Ethical theories: Virtue ethics, utilitarianism, deontology." *Philosophos* [Online]. Available: <https://www.philosophos.org/ethical-theories-virtue-ethics-utilitarianism-deontology>. [Accessed: 2-May-2025].
- [3] M. Manjikian, "Cybersecurity Ethics: An Introduction". *Routledge*, 2017.
- [4] L. Floridi and M. Taddeo, "What is data ethics?" *Philos. Trans. R. Soc. A: Math., Phys. Eng. Sci.*, vol. 374, no. 2083, Art. no. 20160360, 2016.
- [5] Association for Computing Machinery, "ACM Code of Ethics and Professional Conduct." [Online]. Available: <https://www.acm.org/code-of-ethics>. [Accessed: 2-May-2025].
- [6] (ISC)<sup>2</sup>, "Code of Ethics." [Online]. Available: <https://www.isc2.org/Ethics>. [Accessed: 5-May-2025].
- [7] Information Systems Audit and Control Association (ISACA), "Code of Professional Ethics." [Online]. Available: <https://engage.isaca.org/newenglandchapter/aboutchapter/new-page>. [Accessed: 5-May-2025].
- [8] National Institute of Standards and Technology, *NIST Open Government Plan 2016*. Gaithersburg, MD, USA: NIST, 2016. [Online]. Available: <https://www.nist.gov/document/formattednistopengovernmentplan2016finalpdf>. [Accessed: 7-May-2025].
- [9] UK Cyber Security Council, "Ethical principles for individuals." [Online]. Available: <https://www.ukcybersecuritycouncil.org.uk/ethics/ethical-principles-for-individuals/>. [Accessed: 12-May-2025].
- [10] UK Cyber Security Council, "Ethical declaration." [Online]. Available: <https://www.ukcybersecuritycouncil.org.uk/ethics/ethical-declaration/>. [Accessed: 12-May-2025].
- [11] EDUNINE 2025, "IEEE policies: Code of Ethics." [Online]. Available: <https://edunine.eu/edunine2025/eng/ieeePolicies.php#codeE>. [Accessed: 12-May-2025].
- [12] B. Curtis, B. Hefley, and S. Miller, "*People Capability Maturity Model (P-CMM)*, Version 2.0". Pittsburgh, PA, USA: Software Engineering Institute, pp. 1–533, 2009.
- [13] T. L. Saaty, "A scaling method for priorities in hierarchical structures," *J. Math. Psychol.*, vol. 15, no. 3, pp. 234–281, 1977.
- [14] İ. Avcı and M. Koca, "A novel security risk analysis using the AHP method in smart railway systems," *Appl. Sci.*, vol. 14, no. 10, Art. no. 4243, 2024.
- [15] A. J. S. Rojas, E. F. P. Valencia, J. Armas-Aguirre, and J. M. M. Molina, "Cybersecurity maturity model for the protection and privacy of personal health data," in *Proc. 2022 IEEE 2nd Int. Conf. Adv. Learning Technol. Educ. & Res. (ICALTER)*, pp. 1–4, Nov. 2022.
- [16] A E. David, "An ethical framework for cybersecurity professionals: A grounded theory study," *Ph.D. dissertation, Northcentral Univ.*, Prescott, AZ, USA, 2022.
- [17] B. Sadeghi, D. Richards, P. Formosa, M. McEwan, M. H. A. Bajwa, M. Hitchens, and M. Ryan, "Modelling the ethical priorities influencing decision-making in cybersecurity contexts," *Organ. Cybersecurity J.: Pract., Process People*, vol. 3, no. 2, pp. 127–149, 2023.
- [18] N. Sjinin and G. White, "The Community Cyber Security Maturity Model," in *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, Cham, Switzerland: Springer Int. Publishing, pp. 161–183, 2016.
- [19] A. M. Rea-Guaman, T. San Feliu, J. A. Calvo-Manzano, and I. D. Sanchez-Garcia, "Comparative study of cybersecurity capability maturity models," in *Proc. 17th Int. Conf. Software Process Improvement and Capability Determination (SPICE)*, Palma de Mallorca, Spain, Oct. 4–5, pp. 100–113, 2017.
- [20] ISO.org, "ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements." [Online]. Available: <https://www.iso.org/standard/27001>. [Accessed: 18-Oct-2025].
- [21] Türk Standardları Enstitüsü (TSE), "TS EN ISO/IEC 27001 Information Security Management System (Management Systems Certification)." [Online]. Available: <https://www.tse.org.tr/bilgi-guvenligi-yonetim-sistemi-bgys-belgelendirmesi-ts-iso-iec-27001/>. [Accessed: 18-Oct-2025].
- [22] T.C. Cumhurbaşkanlığı, "Bilgi ve İletişim Güvenliği Tedbirleri ile İlgili 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi [Presidential Circular No. 2019/12 on Information and Communication Security Measures]," [Online]. Available: <https://www.lexpera.com.tr/resmi-gazete/metin/bilgi-ve-iletisim-guvenligi-tedbirleri-ile-ilgili-2019-12-sayili-cumhurbaskanligi-genelgesi-30823-1>. [Accessed: 18-Oct-2025]. [in Turkish]
- [23] T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, "Bilgi ve İletişim Güvenliği Denetim Rehberi [Information and Communication Security Audit Guide]," [Online]. Available: [https://ms.hmb.gov.tr/uploads/2021/12/BG\\_Denetim\\_Rehberi-1.pdf](https://ms.hmb.gov.tr/uploads/2021/12/BG_Denetim_Rehberi-1.pdf). [Accessed: 18-Eki-2025]. [in Turkish]
- [24] T.C. Ulaştırma ve Altyapı Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028 [National Cybersecurity Strategy and Action Plan 2024-2028]," [Online]. Available: <https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf>. [Accessed: 18-Oct-2025]. [in Turkish]
- [25] P. Formosa, M. Wilson, and D. Richards, "A principlist framework for cybersecurity ethics," *Computers & Security*, vol. 109, Art. no. 102382, 2021.

- [26] I. Flechais and G. Chalhoub, “Practical cybersecurity ethics: mapping CyBOK to ethical concerns,” in *Proc. 2023 New Security Paradigms Workshop (NSPW)*, pp. 62–75, Sep. 2023.
- [27] M. S. Nasir, H. Khan, A. Qureshi, A. Rafiq, and T. Rasheed, “Ethical aspects in cyber security: Maintaining data integrity and protection: A review,” *Spectrum Eng. Sci.*, vol. 2, no. 3, pp. 420–454, 2024.
- [28] N. Al-Hashem and A. Saidi, “The psychological aspect of cybersecurity: understanding cyber threat perception and decision-making,” *Int. J. Appl. Mach. Learn. Comput. Intell.*, vol. 13, no. 8, pp. 11–22, 2023.
- [29] A. A. G. Navdeep and V. S. Muskan, “The role of ethics in developing secure cyber-security policies,” *Tuijin Jishu J. Propuls. Technol.*, 2023.
- [30] S. Bıçakçı, F. D. Ergun, and M. Çelikpala, “Türkiye’de siber güvenlik [Cybersecurity in Türkiye],” *Ekonomi ve Dış Politika Araştırma Merkezi (EDAM), Siber Politika Kağıtları Serisi*, no. 1, pp. 1–35, 2015. [in Turkish]
- [31] Anadolu Ajansı, “E-Devlet Kapısı’ndan dijital altyapılarından veri sızıntısı iddialarına ilişkin açıklama [Statement on allegations of data leakage from e-Government Gateway digital infrastructures],” Anadolu Ajansı, 27-Oct-2021. [Online]. Available: <https://www.aa.com.tr/tr/gundem/e-devlet-kapisindan-dijital-altyapilarindan-veri-sizintisi-iddialarina-iliskin-aciklama/>. [Accessed: May-15-2025]. [in Turkish]
- [32] Ö. Kutlu and S. Kahraman, “An Analysis of Personal Data Protection Policy in Turkey,” *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi*, vol. 5, no. 4, pp. 45–62, 2017.
- [33] H. Yeşilyurt, “Cyber Security Risks and Solutions in the Financial Services Sector: Payment Systems and Supply Chain Integrity,” *Celal Bayar Univ. Sos. Bilimler Dergisi*, vol. 13, no. 2, pp. 97–120, 2015.
- [34] H. Çakır and M. Taşer, “Evaluation of Cyber Security Activities and Training Studies in Turkey,” *Gazi Univ. J. Sci. Part C: Design Technol.*, pp. 1–1, 2023.
- [35] İ. Avcı and M. Koca, “Cybersecurity attack detection model using machine-learning techniques,” *Acta Polytech. Hung.*, vol. 20, no. 7, pp. 29–44, 2023.
- [36] Anadolu Ajansı, “TürkNet’ten siber saldırı açıklaması [TurkNet’s statement on cyberattack],” Anadolu Ajansı, Apr-15-2025. [Online]. Available: <https://www.aa.com.tr/tr/bilim-teknoloji/turknetten-siber-saldiri-aciklamasi/3508607>. [Accessed: 16-May-2025].
- [37] İ. Avcı, “Investigation of cyber-attack methods and measures in smart grids,” *Sakarya Univ. J. Sci.*, vol. 25, no. 4, pp. 1049–1060, 2021.
- [38] B. Ren, Q. Zhang, J. Ren, S. Ye, and F. Yan, “A novel hybrid approach for water resources carrying capacity assessment by integrating fuzzy comprehensive evaluation and analytical hierarchy process methods with the cloud model,” *Water*, vol. 12, no. 11, p. 3241, 2020.

## Article Information Form

### Authors Contributions

Cevat Özarpa: Conceptualization, Methodology, Investigation, Formal Analysis, Writing – Original Draft, Visualization. İsa Avcı: Conceptualization, Methodology, Resources, Validation, Writing – Review & Editing. Yahya Zakrya Khan: Conceptualization, Methodology, Software, Data Curation, Writing – Review & Editing.

### Conflict of Interest Notice

No conflict of interest regarding the publication of this paper.

### Ethical Approval

Ethics approval was not required for this study as it involved no collection of personal or identifiable data. The survey focused solely on professional perceptions of ethical values, and all participation was voluntary and fully anonymous. The study was conducted in accordance with the principles of academic integrity and ethical research practice.

### Artificial Intelligence Statement

No artificial intelligence tools were used while writing this article.

### Plagiarism Statement

This article has been scanned by iThenticate™.