Медіафорум : аналітика, прогнози, інформаційний менеджмент.
Том 17. 328-346

Mediaforum: Analytics, Forecasts, Information Management.
Volume 17. 328-346

https://doi.org/10.31861/mediaforum.2025.17.328-346
УДК: 004.738.5:[37.01:327]

© *Pavlo Burdiak*[1]

HUMAN FACTOR IN CYBERSECURITY: CYBER EDUCATION AS A SYSTEMIC RESPONSE TO GROWING THREATS IN THE DIGITAL SPACE OF UKRAINE AND THE EU[2]

This article addresses a critical vulnerability in contemporary cybersecurity defenses: the persistent dominance of human factors as the primary vector in successful cyberattacks across Ukraine, the European Union, and globally, despite substantial investments in technical security infrastructure. Empirical evidence from authoritative sources, including Verizon, the World Economic Forum, CERT-UA, and ENISA, consistently identifies that most cybersecurity breaches involve human elements encompassing insider errors and psychological manipulation, with phishing and social engineering accounting for the majority of intrusion entry points. Ukraine's decade-long trajectory of escalating cyber threats – from the 2014 Crimea operations through the catastrophic 2017 NotPetya campaign to sustained high-tempo operations during Russia's 2022–2025 full-scale invasion – demonstrates that adversaries systematically exploit human cognitive vulnerabilities rather than relying exclusively on technical sophistication. Similarly, the European Union faces a diverse threat landscape affecting critical infrastructure. This article argues that cybersecurity policy and practice exhibit a strategic misalignment: while technical defenses have matured substantially, educational frameworks addressing human behavioral vulnerabilities remain fragmented, episodic, and sometimes disconnected from real-world attack patterns. The article frames cybersecurity education not as a mere

[1] PhD student at the Czech Law and Advanced Technologies Research Institute of the Faculty of Law of the Palacký University Olomouc. Email: pavlo.burdiak01@upol.cz; https://orcid.org/0009-0007-0319-5412.

[2] The present article was written by the author within the framework of the EnCycLEd Erasmus+ Project (Nr. 2023-1-AT01-KA220-SCH-000166888). The EnCycLEd Erasmus+ Project is co-funded by the European Union. Views and opinions expressed are however those of the author only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

technical skill domain but as a fundamental dimension of digital citizenship and organizational resilience. It presents the EnCycLEd Erasmus+ project – a cross-border educational initiative that brings together partners from five European countries (Germany, Austria, Greece, Malta, and Ukraine) – as a concrete implementation model demonstrating how cybersecurity literacy can be mainstreamed into general school curricula through interactive, story-driven, age-segmented educational resources grounded in pedagogy and real-world threat patterns. The article employs multi-method research combining quantitative threat intelligence analysis, previous cyber incident narrative analysis, threat landscape characterization, and case study examination to establish that human-centered cybersecurity education constitutes a necessary complement to technical defenses and a strategic policy imperative for institutional and societal resilience in an interconnected digital environment.

Keywords: *cybersecurity, cybersecurity education, Ukraine, EU, human factor, digital resilience, EnCycLEd, CERT-UA, ENISA.*

Людський фактор в кібербезпеці: кіберосвіта як системна відповідь на зростаючі загрози в цифровому просторі України та ЄС

Автор досліджує людський фактор як критичну вразливість сучасної системи кіберзахисту. Попри значні інвестиції в технічні аспекти цифрової безпеки, людський фактор залишається основною причиною успішних кібератак в Україні, ЄС і світі. Дані Verizon, Світового економічного форуму, CERT-UA та ENISA систематично підтверджують, що більшість кіберінцидентів пов'язані з помилковими діями людей та психологічними маніпуляціями. Фішинг та соціальна інженерія є основними способами, які зловмисники використовують для проникнення в інформаційні системи.

Досвід України протягом останнього десятиліття – від кібератак у Криму 2014 року і атаки NotPetya 2017 року до інтенсивних кібероперацій під час повномасштабної російської агресії 2022–2025 років – чітко демонструє: зловмисники свідомо експлуатують не лише технічні прогалини у системах кіберзахисту, а й когнітивні вразливості людей. Аналогічна ситуація спостерігається й у Європейському Союзі, де критична інфраструктура стикається з різноманітними кіберзагрозами, багато з яких здійснюються методами соціальної інженерії.

Стаття викриває стратегічний дисбаланс у сучасних практиках кібербезпеки: хоча технічні рішення значно розвинулися, система освіти в цій сфері залишається фрагментарною, епізодичною та подекуди далекою від реальних моделей кібератак. Автор розглядає кіберосвіту, особливо змалечку, не просто як набір технічних навичок, а як фундаментальний компонент стійкості цифрового суспільства.

Erasmus+ проєкт EnCycLEd служить конкретним прикладом, як цифрова грамотність може бути інтегрована у шкільні навчальні програми через інтерактивні та наративні освітні матеріали, адаптовані під різні вікові категорії учнів, засновані на сучасних практиках викладання та реальних прикладах загроз у кіберпросторі.

Використовуючи комплексний методологічний підхід – від кількісного аналізу даних про кіберзагрози до вивчення кіберінцидентів та конкретних освітніх проєктів з кібербезпеки – стаття наголошує: освіта з цифрової грамотності і опанування найкращих практик кібербезпеки є важливою складовою забезпечення інституційної та соціальної стійкості в цифровому світі. Тому кіберосвіта повинна доповнювати технічні засоби захисту інформаційних систем.

Ключові слова: *кібербезпека, освіта з кібербезпеки, Україна, ЄС, людський фактор, цифрова стійкість, EnCycLEd, CERT-UA, ENISA.*

Formulation of the scientific problem and its significance. The scientific problem addressed in this article concerns the nexus between escalating cybersecurity threats in Ukraine and the EU and the insufficient integration of human-centered cybersecurity education as a foundational defense mechanism across institutional and societal levels. The article identifies a critical paradox: while advanced technical defenses continue to proliferate, the human factor remains the dominant vulnerability in cybersecurity incidents, accounting for 68–95% of all breaches globally (World Economic Forum, 2022; Verizon, 2024). This paradox is particularly acute in geopolitically contested regions and rapidly digitizing societies where hybrid warfare blends cyberattacks with kinetic military operations, disinformation campaigns, and psychological manipulation.

The significance of this problem extends across multiple dimensions. Firstly, empirical urgency: Ukraine's cyber threat environment demonstrates a decade-long escalation trajectory, culminating in 4315 registered cyber incidents in 2024 alone – an almost 70% year-on-year increase (State Service of Special Communications and Information Protection of

Ukraine, 2024) – while the European Union confronts a diverse and converging threat landscape affecting critical infrastructure across public administration (38.2% of incidents), transport, and digital services (ENISA, 2025).

Secondly, strategic misalignment: technical defenses have matured substantially, yet organizational vulnerability derives not from the absence of firewalls or encryption, but from the persistent human vulnerabilities exploited through phishing, social engineering, and psychological manipulation.

Thirdly, educational vacuum: despite recognition of the human factor as the critical vulnerability, mainstream cybersecurity education remains fragmented, episodic, and often disconnected from real-world attack patterns, leaving both school-age populations and working professionals underprepared for the social engineering techniques they actually encounter.

The article frames cybersecurity education not merely as a technical skill domain but as a fundamental dimension of digital citizenship and resilience – a systemic response mechanism grounded in pedagogical science and real-world threat awareness. This framing aligns cybersecurity literacy with foundational competencies such as reading and numeracy, acknowledging that in an interconnected digital environment, human judgment, habit formation, and threat recognition constitute irreplaceable layers of defense.

Analysis of recent research on this problem. Recent authoritative studies establish the empirical foundation for the article's core claims. The Verizon 2024 Data Breach Investigations Report, analyzing a number of security incidents and verified breaches, documents evidence that human elements – encompassing both insider errors and successful social engineering campaigns – constitute a predominant proportion of breaches globally (Verizon, 2024). The World Economic Forum's Global Risks Report corroborates these findings through the analysis of cybersecurity incident causation, identifying human error as a significant causal factor across diverse organizational and sectoral contexts (World Economic Forum, 2022).

Building upon this international research foundation, contemporary Ukrainian scholarship deepens understanding of the human factor within the specific context of hybrid warfare. Pavlo Burdiak's analysis «A Malicious Alliance: How Cyberattacks and Disinformation are Synchronously Destabilizing the Digital Space of Ukraine in the Face of Russian Aggres-

sion» examines the symbiotic relationship between cyber operations and information manipulation, demonstrating how adversaries coordinate technical attacks with psychological operations to amplify disruptive effects. This work highlights the operational integration of cyberattacks and disinformation as complementary tools within a unified strategic framework, rather than discrete threat vectors (Burdiak, 2024).

Complementing this strategic analysis, the scientific article «From Awareness to Management: A Concept of Human Risks in the Cybersecurity System» authored by Lesya Kozubtsova, Valery Lishchyna, and Igor Kozubtsov addresses the psychological and pedagogical dimensions of the human factor in information and cybersecurity contexts. This research work develops conceptual frameworks for understanding human risk management as a distinct category, separate from traditional security awareness training, and argues that managing risks associated with human behavior promises greater return on investment than other strategic security initiatives (Козубцова, Ліщина, і Козубцов, 2025).

Ukrainian research on threat characterization is further advanced through the work of Horun, whose analysis «Cybersecurity Threats to Ukraine in the Context of Russian Aggression» examines emerging threat vectors, information-psychological impact mechanisms, and technical interference in IT systems within Ukraine's wartime environment. This scholarship characterizes contemporary attack types, identifies their most dangerous consequences, and analyzes the operational structures and cooperation problems underlying cyber defense countermeasures within Ukraine's cyberspace during the ongoing conflict (Горун, 2025).

The present article contributes to this literature by explicitly linking Ukrainian and EU threat data and human-factor research to a concrete educational initiative (EnCycLEd) that aims to mainstream cybersecurity literacy in schools through interactive, story-based content.

Formulation of the purpose, objectives, and methods of the article. The article's overarching purpose is to articulate cybersecurity education as a strategic and systemic response to the demonstrated gap between technical defenses and human vulnerability, with particular emphasis on school-based implementation as a foundational intervention point that reaches young people before labor market entry while creating family-level spillover effects through student-mediated learning activities.

To achieve this purpose, the article sets the following objectives:

1. Summarise key characteristics of the cyber threat environment in Ukraine.
2. Outline the main cyber threats and trends in the EU as identified by ENISA.
3. Analyse empirical evidence regarding the centrality of the human factor in cyber incidents in Ukraine, EU, and worldwide.
4. Present the EnCycLEd Erasmus+ project as a concrete implementation model demonstrating how abstract principles of cybersecurity literacy can be operationalized into interactive, classroom-ready, cross-border, age-segmented educational resources that integrate behavioral insights and real-world threat patterns.

With regard to methodology, the article employs a multi-method research approach combining quantitative threat intelligence analysis, qualitative cyber incidents analysis, and case study examination:

1. Quantitative threat intelligence analysis. The article synthesizes published incident statistics from CERT-UA (Ukraine's national cybersecurity authority), ENISA (the European Union Agency for Cybersecurity), and commercial security firms to establish volumetric trends, sectoral vulnerability patterns, and severity distributions. These statistics provide empirical grounding for claims about escalation, convergence, and the persistence of human-factor exploitation.

2. Previous cyber incidents analysis. The article traces major cyber incidents in Ukraine – the 2014 Crimea operations, the 2015 power grid attack, the 2017 NotPetya campaign, and 2022–2024 operations during Russia's full-scale invasion – to establish historical continuity in attack patterns, operational templates for integrating cyber and kinetic warfare, and the progressive sophistication of adversary tradecraft. This historical perspective contextualizes current threats as manifestations of evolving strategies rather than isolated incidents.
3. Threat landscape analysis. The article examines threat patterns, actor categories, sectoral targeting, and attack methodologies across Ukraine and the European Union to identify both context-specific vulnerabilities and generalizable threat patterns. This approach acknowledges distinct geopolitical circumstances while identifying common human-factor exploitations that transcend national boundaries.
4. Case study examination. The article presents EnCycLEd as a bounded case study demonstrating operationalization of cybersecurity

education principles in school, incorporating age-segmented curricula (10–14 and 15–18 age groups) and interactive learning modules.

The article's analytical framework rests on three foundational propositions:

1. Human vulnerability proposition. Human cognitive and behavioral vulnerabilities constitute the dominant vector in cybersecurity incidents, not technical system failures. This proposition directs analytical focus toward psychological mechanisms – trust exploitation, cognitive biases, social proof – rather than exclusive emphasis on technical exploits.

2. Behavioral change proposition. Behavior change in cybersecurity requires sustained, age-appropriate, interactive education grounded in psychological principles of motivation, ability, and situational prompts, rather than episodic compliance training. This proposition justifies emphasis on gamification, scenario-based learning, and feedback mechanisms, as suggested by the EnCycLEd project.

3. Educational integration proposition. Cybersecurity literacy constitutes a transversal competence – fundamental to modern citizenship – that should be integrated into diverse subject domains (civic studies, home economics, communication, not just IT) through teacher training and resource provision, rather than confined to specialist technical programs.

This multi-method, evidence-grounded approach positions the article within contemporary interdisciplinary scholarship addressing cybersecurity not as a technical domain but as a sociotechnical system in which human behavior, organizational culture, pedagogical design, and policy frameworks operate as interconnected components requiring coordinated intervention.

Presentation of the main material. Cybersecurity challenges in Ukraine. Ukraine's contemporary cyber threat environment cannot be understood as a sudden by-product of the full-scale invasion that began in February 2022. It is the outcome of a decade-long trajectory in which cyber operations progressively complemented coercion, covert action, and information manipulation in Russia's campaign against Ukrainian sovereignty. Scholarship and policy analysis commonly locate a structural shift around the Euromaidan protests (2013–2014) and Russia's subsequent illegal annexation of Crimea and military intervention in eastern Ukraine, after which cyber incidents connected to the conflict increased markedly (Burdiak, 2019).

During the illegal annexation of Crimea in February–March 2014, Russian state-sponsored actors synchronized cyber operations with military maneuvers to facilitate territorial seizure (Burdiak, 2019). Hackers supposedly affiliated with and/or acting in the interest of Russia conducted DDoS attacks shutting down Ukrainian computer networks and communications (Przetacznik and Tarpova, 2022), compromised mobile phones of parliamentary deputies (Polityuk and Finkle, 2014), and executed network jamming (Harris, 2014) to disrupt governmental coordination. These cyber operations created temporal advantage by delaying Ukrainian responses while Russia completed military seizure through conventional means, establishing an operational template for integrating cyber and kinetic warfare (Burdiak, 2019).

The December 2015 power grid attack marked a shift from disruption of information systems to demonstrable effects on critical infrastructure and civilian life. On 23 December 2015, attackers used spear phishing-led intrusion paths and then moved into operational environments to disrupt electricity distribution. Cyber attacks were directed at regional electric power distribution companies (Oblenergos), causing power outages affecting about 225,000 customers (CISA, 2021). This was regarded as the first known successful cyber attack on an electrical grid (BBC, 2016).

During the 2016–2021 period, cyberattacks targeting Ukraine escalated substantially in both frequency and sophistication. The June 2017 NotPetya malware campaign represented arguably one of the most destructive cyber operation in recorded history (HYPR, n.d.). It infected thousands of organizations globally, with the vast majority of victims located in Ukraine. Unlike traditional ransomware designed to extract financial payment, NotPetya was primarily destructive – it encrypted entire hard disks and permanently wiped files with no possibility of recovery. The malware was spreading rapidly across networks without requiring user intervention. Although NotPetya displayed a ransom message, it contained a fake Bitcoin address, suggesting the attackers' true objective was destruction rather than financial gain. In 2018, several nations attributed the NotPetya attacks to the Russian government, indicating that the campaign likely had geopolitical motivations beyond typical cybercriminal profit motives. This distinction – combining wiper malware functionality with the appearance of ransomware – made NotPetya a watershed moment in cyberattack strategy, demonstrating how malware could be weaponized for destructive rather than purely financial purposes (Cloudflare. n.d.).

Following the 2022 full-scale Russian invasion of Ukraine, cyberwarfare elevated to a different level. CERT-UA's published statistics show a sharp rise in the total number of registered cyber incidents over time, with a particularly notable jump in 2024. The reported totals are 1350 cyber incidents (in 2021), 2194 (2022), 2543 (2023), and 4315 (2024). This pattern supports an interpretation of intensifying activity, but it also plausibly reflects improved detection, reporting, and institutional capacity, especially given Ukraine's accelerated cybersecurity partnerships since 2022 (State Service of Special Communications and Information Protection of Ukraine, 2024).

The same CERT-UA materials indicate a divergence between volume and destructive severity. «Critical and high-severity» incidents are make up a total of 403 incidents (in 2021), 1048 (2022), 367 (2023), and 59 (2024). Within 2024, a semester comparison shows total incidents rising from 1739 (H1) to 2576 (H2), while critical incidents decreased from 3 to 1 and high-severity incidents decreased from 45 to 10 (State Service of Special Communications and Information Protection of Ukraine, 2024). This is a substantial decrease in high/critical-severity incidents alongside rising overall incident counts.

Academically, this combination can be interpreted in at least three non-exclusive ways. First, it may indicate that defenders improved resilience and response, containing more events before they escalated into disruptive or destructive outcomes. Second, it may reflect a shift by adversaries toward scalable, «good enough» techniques (mass phishing and malware distribution) that generate many incidents but fewer immediate catastrophic impacts. Third, it may reveal classification dynamics: as monitoring improves, more medium- and low-severity events are captured and triaged, increasing totals while diluting the proportion of severe cases. The data itself does not prove which mechanism dominates, but it does justify a key claim: escalation in hostile cyber pressure does not necessarily translate into proportional escalation in realized damage if defensive capacity and detection rise in parallel.

More recently, public reporting of CERT-UA in 2025 emphasizes the persistence of a high-tempo threat environment and the continued centrality of Russian-origin activity, alongside additional activity from other jurisdictions. Since the beginning of 2025, CERT-UA recorded on average around 15 cyber incidents per day and tracked more than 150 cyber threat clusters (UAC). This aligns with the broader picture provided by 2024 sta-

tistics: sustained high volume, frequent phishing and malware distribution, and persistent espionage priorities (Державна служба спеціального зв'язку та захисту інформації України, 2025).

The same reporting emphasizes four broad categories of adversary activity (Державна служба спеціального зв'язку та захисту інформації України, 2025):

- espionage (particularly in the field of defense);
- sabotage/cyberterrorism affecting everyone's life;
- financially motivated crime (aimed at stealing money);
- niche campaigns against specific professional groups.

In practice, Ukraine faces a crowded ecosystem in which state-aligned groups, proxies, and financially motivated actors coexist, sometimes sharing tactics, infrastructure, or opportunity structures created by wartime disruption to perpetrate cyberattacks.

The CEDEM study «A Malicious Alliance» complements this picture by analysing five concrete attack patterns that combine cyber and information dimensions: cloning of news websites, hacking of media portals, DDoS against information resources, jamming of satellite signals, and phishing schemes that masquerade as social payments, Meta community rule violations, security alerts, etc. In each case, cyberattacks are used to deliver disinformation or to disable trusted channels, amplifying psychological impact (Burdiak, 2024).

Cybersecurity challenges in the European Union. The European Union confronts an escalating cyber threat landscape characterized by operational sophistication and strategic impact. The European Union Agency for Cybersecurity (ENISA) released a 2025 Threat Landscape report, in which ENISA analysts systematically collected and analyzed 4875 cyber incidents spanning the period from July 2024, to June 2025 (ENISA, 2025). Based on the said report, this chapter sheds light on principal cybersecurity challenges confronting the European Union through analysis of dominant attack typologies, sectoral vulnerability patterns, and strategic threat vectors, establishing the empirical foundation for understanding contemporary European cyber risks.

The contemporary cyber threat landscape targeting the European Union exhibits sharply skewed incident distribution. Distributed denial-of-service (DDoS) attacks constitute the overwhelmingly predominant incident category, accounting for 76.7% of all recorded incidents during the reporting period. This extraordinary concentration reflects the operational

preferences of hacktivist threat actors (primarily responsible for the vast majority of documented DDoS incidents), who deploy DDoS attacks as primary tactical mechanisms for conducting politically motivated disruption campaigns (ENISA, 2025).

Intrusions constitute the second major incident category, accounting for 17.8% of all documented incidents. In contrast to DDoS operations, intrusions are predominantly executed by cybercriminal operators seeking to establish unauthorized network access for data exfiltration and financial exploitation, followed secondarily by state-aligned intrusion sets pursuing, inter alia, persistent network presence for strategic intelligence collection and operational access. Hacktivist groups appear only marginally within intrusion incident data, reflecting their operational emphasis upon high-visibility disruption tactics rather than sophisticated network persistence attack methodologies (ENISA, 2025).

The malicious code deployed following successful cybercriminal-led intrusions reveals the dominant objectives and financial motivations underlying cybercriminal operations. Ransomware, banking trojans, and information-stealing malware collectively comprise 87.3% of malware deployed following these intrusions, reflecting cybercriminal concentration upon either encryption-based extortion or direct financial fraud and data theft. The outcomes of recorded intrusions further substantiate financially motivated threat actor prevalence: 68.6% of documented intrusions resulted in data breaches with stolen information subsequently marketed on cybercriminal forums for resale, including 2.8% of breached datasets explicitly advertised as products of ransomware extortion operations. Data exfiltration following intrusions, encompassing both credential theft (8.9%) and strategic data collection for subsequent exploitation (21.3%), accounts for an additional 30.2% of documented intrusion outcomes. The cumulative pattern demonstrates that financial extraction through data theft and ransom extortion constitute the primary operational motivations underlying cybercriminal intrusion campaigns (ENISA, 2025).

Public administration emerges as the most extensively targeted sectoral domain within the European Union, accounting for 38.2% of all recorded cyberattacks. Transport and logistics constitute the second most targeted sector, accounting for 7.5% of documented incidents. Digital infrastructure and services, comprising telecommunications operators, cloud service providers, content delivery networks, and internet backbone operators, remains substantially targeted (4.8%) despite lower numerical incident

counts. Digital infrastructure constitutes disproportionately high-value targets due to inherent cyber dependencies – compromises of foundational digital infrastructure create cascading impacts affecting thousands of dependent organizations and services (ENISA, 2025).

The human element in cybersecurity incidents. Empirical evidence converges across Ukraine, the European Union, and the global cybersecurity context on a counterintuitive yet pivotal conclusion: the human factor constitutes the dominant vector in cybersecurity incidents, superseding technical vulnerabilities and sophisticated exploit techniques as the primary mechanism enabling successful cyberattacks.

The Verizon 2024 Data Breach Investigations Report (DBIR), analyzing 30458 security incidents and 10626 verified breaches in 2023, documents that 68% of data breaches involve a non-malicious human element encompassing insider errors and successful social engineering campaigns; if malicious insider actions are included, the human factor accounts for approximately 76% of all breaches (Verizon, 2024).

The World Economic Forum, through its annual Global Risks Report, identifies that 95% of all cybersecurity incidents occur due to human error. This statistic reflects the structural reality that even the most advanced technical defenses remain vulnerable to exploitation through human cognitive and behavioral weaknesses that can be misused by malicious actors (World Economic Forum, 2022).

Within the Ukrainian context, CERT-UA observes that the compromise chain for various cyber threats remains relatively unchanged: phishing emails containing malicious attachments constitute the primary initial access mechanism (Державна служба спеціального зв'язку та захисту інформації України, 2025). Contemporary hybrid warfare evidence from Ukraine demonstrates that adversaries obtain approximately 90% of operationally significant intelligence through social engineering conducted via social media platforms, including Facebook, Telegram, Instagram, WhatsApp, and YouTube (Козубцова, Ліщина, і Козубцов, 2025), indicating that technical security controls cannot compensate for human cognitive vulnerabilities when adversaries leverage psychological manipulation and trust exploitation.

In the EU context, as reported by ENISA, a social engineering method – phishing – remained the primary initial access method for cyberattacks, accounting for approximately 60% of observed intrusion entry points and spanning multiple modalities, including malicious email campaigns (mal-

spam), voice-based social engineering (vishing), and malicious advertising (malvertising) (ENISA, 2025).

The pervasiveness of the human factor across diverse geopolitical, sectoral, and organizational contexts establishes cybersecurity not only as a technical issue but fundamentally as a human behavioral and organizational cultural challenge requiring interventions grounded in psychological understanding, behavioral change theory, and educational methodology rather than disproportionate reliance upon technological solutions.

Cybersecurity education as a systemic response. If the weakest link in cybersecurity is indeed «between the keyboard and the chair», then strengthening that link requires more than occasional reminders. It requires sustained, age-appropriate education that develops knowledge, habits and a sense of shared responsibility in the digital domain.

From a policy perspective, several lines of action are apparent. First, cybersecurity should be integrated into general digital literacy and civic education, rather than confined to specialist programmes. Second, educational content must reflect real attack patterns, including phishing, ransomware, and social media manipulation, so that learners can connect abstract concepts with familiar situations. Third, education must be designed with behavioural insights in mind, using interactive stories, simulations, and gamification (Bötticher, 2024).

Traditional lecture-based awareness often fails to change behaviour. By contrast, interactive methods such as scenario-based discussions, games, role-playing and peer-to-peer teaching can help students internalise both threats and defences.

For Ukraine and the EU alike, schools are a strategic point of intervention. They can equip young people with cyber hygiene skills before they enter the labour market, while also reaching families indirectly through assignments and projects that involve parents. The EnCycLEd Erasmus+ project provides a concrete model of how this can be done.

The EnCycLEd Erasmus+ project as a case study. In light of the symbiotic relationship between cyber threats and human vulnerability, it becomes clear that technical defenses must be augmented by a robust educational framework. This is the mission of the EnCycLEd project («Enhancing Cybersecurity Literacy in Education»). Co-funded by the European Union under the Erasmus+ program, EnCycLEd represents a strategic effort to inoculate the next generation against the digital threats described above.

EnCycLEd operates on the premise that cybersecurity is a transversal competence, as fundamental to modern citizenship as reading or mathematics. The project, running from 2023 to 2026, brings together a consortium of partners from five countries: Germany, Austria, Ukraine, Greece, and Malta. This geographic diversity is strategic, allowing the project to draw on the experiences of the EU countries while integrating the frontline, battle-hardened cybersecurity experiences of Ukrainian partners.

The core objective of EnCycLEd is to «mainstream» cybersecurity education. It rejects the notion that cyber safety is the sole domain of IT specialists. Instead, it aims to equip school teachers and educators in training with a toolkit that can be integrated into diverse subjects – from Civic Studies (discussing disinformation and democracy) to Home Economics (discussing IoT security in smart homes) and Communication classes, etc.

The project's output is structured around five Work Packages, culminating in a set of tangible educational resources hosted on the multilingual EnCycLEd Platform (go.encycled.eu).

The EnCycLEd curriculum is divided into five modules, designed for two age groups: 10–14 years and 15–18 years. This segmentation acknowledges the different cognitive developmental stages and digital usage patterns of these groups. The modules are as follows:

– Module 1: «What is cybersecurity?» introduces basic notions of online safety and cybersecurity in an accessible language, explaining concepts such as cybersecurity, cyberattack, etc.

– Module 2: «Who was it?» presents a narrative about a ransomware attack on a municipality. Through the story, students learn about ransomware, incident response, and the «disclosure dilemma» regarding whether and how to inform the public about cyber incidents.

– Module 3: «What can we do against it?» focuses on resilience and defence. A key component is the online game «Cyber Crime Time», where learners adopt the role of a white-hat hacker to explore typical attack paths and see how defensive measures can block them.

– Module 4: «Cyber Defender» provides interviews with cybersecurity professionals working in various fields who share their experience with and insights into the domain of digital security, offering advice and serving as inspiration for young students to pursue a career in this field.

– Module 5: «Simulation» engages students in negotiating a «cyber peace document.» It frames cybersecurity not just as a technical issue but

as a diplomatic and geopolitical one, involving multiple stakeholders, and fostering skills in negotiation, ethics, and international relations.

All modules are interactive and story-driven, combining textual explanations, scenarios, worksheets, group discussions and, where appropriate, comics and simple simulations.

In addition, the EnCycLEd platform (https://go.encycled.eu/) hosts a resource repository that aggregates both EnCycLEd-developed materials and carefully curated external resources. The repository includes videos, comics, quizzes, interactive platforms and toolkits on topics such as data protection, password hygiene, phishing, device security, digital footprints and social media risks. Resources are tagged by age group, audience (students, educators, parents) and topic, enabling teachers to identify suitable materials quickly.

Furthermore, EnCycLEd adopts a bidirectional learning approach. It aims not only to train teachers, but also to empower students as «cybersecurity ambassadors» who can raise awareness among peers and in their communities. To this end, the project develops training toolkits, video tutorials, and interviews with cybersecurity experts and industry representatives.

Finally, the platform has a discussion room functionality for vetted students and teachers, which is designed as a safe online environment for national and international peer-to-peer communication, with behaviour policies and abuse reporting mechanisms. It is intended to serve as a space where school students and teachers can share experiences, lesson plans and feedback with each other and with cybersecurity professionals.

As such, EnCycLEd operationalises the abstract call to «raise cyber awareness» by providing concrete, classroom-ready content that addresses real-world threats, integrates behavioural insights and connects schools across borders.

Conclusions. The analysis presented in this article reveals a fundamental structural vulnerability in contemporary cybersecurity practice: the persistent gap between sophisticated technical defenses and the persistent human behaviors that enable successful cyberattacks. The evidence converges across Ukraine, the European Union, and global contexts to establish an incontrovertible fact – the human factor, not just advanced malware or zero-day exploits, constitutes the dominant vector in cybersecurity incidents. This finding demands a strategic reorientation of cybersecurity policy and practice from the emphasis on technical solutions toward

integrated sociotechnical approaches that foreground human behavioral change, psychological resilience, and educational intervention.

Ukraine's experience provides particularly instructive evidence for this reorientation. The nation's over a decade-long trajectory of cyber operations, escalating from the 2014 Crimea operations through the catastrophic 2017 NotPetya campaign to the sustained high-tempo operations of 2022–2025, demonstrates that adversaries have consistently exploited human vulnerabilities – phishing, social engineering, trust exploitation – rather than relying exclusively on technical sophistication. The persistence of phishing as the primary initial access mechanism, accounting for the compromise of Ukrainian systems across all sectors, alongside evidence that approximately 90% of operationally significant intelligence derives from social media-based social engineering, reveals that human judgment and behavioral discipline constitute irreplaceable layers of defense. Similarly, the European Union's threat landscape, dominated by DDoS operations targeting public administration and ransomware targeting critical infrastructure, demonstrates that adversaries prioritize human-accessible entry points – initial access through phishing and social engineering – over sophisticated technical exploitation.

The article's integration of Ukrainian and EU threat data with empirical research on the human factor in cybersecurity incidents (Verizon, World Economic Forum, CERT-UA, and ENISA analyses) establishes that this vulnerability is not a local or sectoral phenomenon but a structural characteristic of digitalized societies. When 68–95% of breaches involve human factors, and 60–90% of intrusions begin through social engineering, the policy implication becomes unavoidable: technical investments alone cannot resolve cybersecurity challenges. Organizational resilience requires complementary investments in human-centered education, behavioral change mechanisms, and systemic cultural transformation.

The EnCycLEd Erasmus+ project, presented in this article as a concrete implementation model, operationalizes this reorientation through a strategic intervention at the critical juncture of formal education. By suggesting the integration of cybersecurity literacy into general curricula for 10–18 year-old students across European countries – including Ukraine – the project embodies several foundational principles that merit generalization:

1. First, educational integration rather than pure technical specialization. EnCycLEd rejects the premise that cybersecurity education belongs exclusively to IT specialists. By providing tools for civic studies teachers,

home economics educators, and communication instructors to integrate cybersecurity concepts into their domains, the project democratizes cyber literacy and positions it as a transversal competence equivalent to reading comprehension or mathematical reasoning.

2. Second, behavioral design that is grounded in pedagogical and psychological insights. The project's incorporation of gamification, story-driven scenarios, interactive simulations, and reflection mechanisms reflects evidence-based principles from behavioral psychology and pedagogy. Rather than relying on fear-based compliance messaging or abstract technical lectures, EnCycLEd employs narrative structures and interactive experiences that activate intrinsic motivation and facilitate habit formation – the mechanisms through which sustained behavioral change may occur.

3. Third, real-world threat relevance. By designing curriculum modules around concrete attack patterns (ransomware attacks on municipalities, phishing schemes masquerading as legitimate services, coordinated cyberattacks), the project ensures that learners connect abstract cybersecurity concepts with familiar, experientially relevant situations. This pedagogical approach addresses a critical failure of traditional awareness training – its disconnection from actual threat vectors that learners encounter.

4. Fourth, cross-border knowledge transfer and solidarity. The inclusion of Ukrainian partners alongside EU member states acknowledges that cybersecurity threats transcend institutional borders and that frontline experiences with hybrid warfare contain valuable insights for societies not currently experiencing active cyberattacks. This approach transforms educational exchange from a unidirectional transfer from «developed» to «developing» contexts into genuine peer learning grounded in practical experience.

Such educational initiatives do not replace technical defenses but rather operationalize the recognition that in an interconnected digital environment, human judgment, behavioral discipline, and shared responsibility constitute irreplaceable layers of resilience. The urgency of this educational transformation cannot be overstated: the alternative is continued escalation of successful cyber incidents, disinformation campaigns, and hybrid warfare operations that exploit predictable human vulnerabilities. The choice between investing in human-centered cybersecurity education and accepting continued erosion of institutional and societal resi-

lience through preventable human-factor exploitation is not genuinely a choice – it is a policy imperative grounded in evidence and geopolitical necessity.

References:

1. BBC. 2016. Hackers behind Ukraine power cuts, says US report. https://www.bbc.com/news/technology-35667989

2. Bötticher, Astrid. 2024. "Evaluating the need for cybersecurity teaching materials for schools". Future Law Working Papers. https://www.uibk.ac.at/media/filer_public/b8/d6/b8d66b87-8128-4909-9847-ae8979e-ab394/flwp_2024_4_final.pdf

3. Burdiak, Pavlo. 2019. "The role of cyber space in the geopolitical confrontation between Ukraine and Russia". Chernivtsi, The materials of XIII International conference for students and young scientists "Foreign policy of Ukraine: current agenda", pp. 24-26. https://drive.google.com/file/d/1tvrWPWN4w4dSrJveZcZ71Io8TylbW_A9/view

4. Burdiak, Pavlo. 2024. "A Malicious Alliance: How Cyberattacks and Disinformation are Synchronously Destabilizing the Digital Space of Ukraine in the Face of Russian Aggression". CEDEM. https://cedem.org.ua/wp-content/uploads/2024/12/CEDEM_cyberdis_eng.pdf

5. CISA. 2021. "Cyber-Attack Against Ukrainian Critical Infrastructure". https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

6. Cloudflare. n.d. What are Petya and NotPetya? Accessed December 1, 2025. https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/

7. ENISA. 2025. "Threat Landscape report 2025." https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025_0.pdf

8. Harris, Shane. 2014. "Hack Attack Russia's first targets in Ukraine: its cell phones and Internet lines." Foreign Policy. https://foreignpolicy.com/2014/03/03/hack-attack/

9. HYPR, n.d. NotPetya. HYPR Encyclopedia. Accessed December 1, 2025. https://www.hypr.com/security-encyclopedia/notpetya

10. Polityuk, Pavel, and Jim Finkle. 2014. "Ukraine says communications hit, MPs phones blocked". Reuters. https://www.reuters.com/article/world/ukraine-says-communications-hit-mps-phones-blocked-idUSBREA231R2/

11. Przetacznik, Jakub, and Simona Tarpova. 2022. "Russia's war on Ukraine: Timeline of cyber-attacks." European Parliament Briefing. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI%282022%29733549_EN.pdf

12. State Service of Special Communications and Information Protection of Ukraine. 2024. "Russian Cyber Operations." https://cip.gov.ua/services/cm/api/attachment/download?id=68768

13. Verizon. 2024. "Data Breach Investigations Report". https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

14. World Economic Forum. 2022. "The Global Risks Report 2022". https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

15. Horun, O. 2025. "Kiberzahrozy Ukrayiny v umovakh ahresiyi RF". Informatsiya i pravo. http://il.ippi.org.ua/article/view/340520 (In Ukrainian).

16. Derzhavna sluzhba spetsial'noho zv'yazku ta zakhystu informatsiyi Ukrayiny. 2025. Ohlyad kiberzahroz ta stratehiy zakhystu v 2025 rotsi: dosvid CERT-UA. https://cip.gov.ua/ua/faqs/cyber-threat-overview-and-defense-strategies-in-2025-cert-ua-s-experience (In Ukrainian).

17. Kozubtsova, Lesya, Lishchyna Valeriy, i Kozubtsov Ihor. 2025. "Vid obiznanosti do upravlinnya: Kontseptsiya lyuds'kykh ryzykiv v systemi kiberzakhystu". Kiberbezpeka: osvita, nauka, tekhnika. https://csecurity.kubg.edu.ua/index.php/journal/article/view/895/810 (In Ukrainian).

Надійшла до редакції / Received: 23.11.2025 *Схвалено до друку / Accepted: 08.12.2025*