SPECTRUM
Journal of Social Sciences

ASPUR PUBLISHING

Vol. 04, No. 02 (2027) 83-94, doi: 10.61552/SJSS.2027.02.001 - http://spectrum.aspur.rs

CYBERSECURITY AND HUMAN TRAFFICKING PROTECTION

Tiana Kaleeva [1]

Received 29.07.2026.
Revised 23.09.2026.
Accepted 19.10.2026.

Keywords:

Human trafficking, cybersecurity, social issues, protection.

Original research





A B S T R A C T

The aim of this article is to outline the existing threat and negative societal effec on security regarding human trafficking, including in cyberspace. The researc emphasizes on the necessity of adequate mechanisms and actions for fightin human trafficking and suspicious online activity. Cyberspace provides bot benefits and drawbacks in combating human trafficking, since it is intensivel applied by traffickers in hunting victims. The research is performed throug documentary and comparative analysis of current human trafficking issue legislative data and existing initiatives in fighting it, as well as a survey amon 84 people in Bulgaria, concerning human trafficking and online security. Th article presents the interconnection between cyberspace, security, and figh against human trafficking.

© 2027 SPECTRUM Journal of Social Sciences

1. INTRODUCTION

Human trafficking (HT) is a crime against human rights, affecting not only separate individuals but also societal wellbeing, public health, safety, political, and economic life on national, regional, and global level. As a form of an organized crime, it is undermining the principles of democracy and rule of law, representing violation against human beings and social development. HT is based on coercion, force or fraud with sole purpose to exploit individuals against their free will through recruitment and involuntary movement (Pajić, 2023).

By its essence, security science incorporates knowledge of security management, build environment, security principles, and security risk management (Smith & Brooks, 2013). Its goal is to formulate a better understanding of security concepts, challenges and instruments for protection. Through efficient security measures the security science aims to overcome difficulties in identifying security weaknesses, potential risks and threats, appropriate security controls, and adequate protection methods.

Since it is a threat to the national security and human safety, to a significant extend HT is considered a crime interrelated to security science. Derived from that, its combating requires an interdisciplinary, multilayer approach, including risk analysis, strategic security prioritization, integrated security programs, systematic technological procedures, etc. Both, successful countering or inability to oppose HT, inevitably affect security and establishment of future mechanisms in fighting this crime.

Many factors pose as a vulnerability to society leading to HT occurrence: weak legal and regulatory framework; corruption in government and law enforcement bodies; economic inequality; low public awareness; cybersecurity and digital capability gaps. As a result, numerous security threats emerge in the form of increased establishment of organized criminal networks, introduction of innovative cross-border trafficking methods, money laundry, new cyber-criminal activities, online recruitment and grooming, etc.

Among main risks regarding HT are differentiated the human right violation, physical violence and abuse.

[1] Corresponding author: Tiana Kaleeva
Email: tianakaleeva@gmail.com

Therefore, growth of organized crime, reduced public safety and increased migration might be observed in a long term. If HT is not mitigated, severe societal consequences would affect national and international security governance, such as: strengthening of organized crime; weakened law and judicial system; public safety hazards; financial crimes; cybersecurity challenges; reduced public trust; international security implications, etc.

HT is not limited to a particular region or exploitation form, which is outlining its significant scale of spreading and necessity of adequate mechanisms for timely and adequately fighting it, as well as enhancing national and international security. It is challenging to statistically determine the scope of HT since the crime is characterized by a hidden nature (Stöckl et al., 2021). In order to estimate the number of victims, their identification and testimonies are required, problematic not only for collection but also for processing and proper analysis.

What is becoming even more challenging is the detection of HT in cyberspace. People face various difficulties in comprehending they are HT victims, therefore to timely report and undertake appropriate actions, leaving them and others vulnerable and unprotected. Consequently, cybersecurity and HT should be considered as interconnected, even more in the contemporary digitalized societies. Moreover, cybersecurity is affected by human factors which are influencing people's interaction with information security systems and human understanding of cybersecurity threats (Kadena & Gupi, 2021).

The current research is performed by the application of four main approaches, justifying the chosen research methods in the article:

- *Documentary approach* – assists the study of HT by conducting bibliographic research founded on reliable information from a variety of domains and technical fields;
- *Systematic approach* – presents comprehensive knowledge on HT challenges, vulnerabilities and security strategies. Through comparative and documentary analysis as scientific methods, the study's purpose is furthered by offering different approaches to the raised problematic area;
- *Process approach* – in accordance to which, effective protection techniques are achieved through a variety of interconnected continuous operations. The process approach supports identification of strategic mechanisms and opportunities for security improvement;
- *Quantitative approach* – its aim is to study quantitative data as an addition to the conducted documentary and comparative analysis in order to emphasize on the connection between cybersecurity and HT. As well as that, the provided questionnaire's purpose is to outline main issues, pointed out by the surveyed respondents, in search for the current actuality of the problematic area.

In addition to theoretically researching previous and current state of HT, based on presented data, legislation and recommendations, the article studies survey data in order to highlight the effect of HT on social wellbeing. The literature is selected in an aim to identify main issues and actions against HT. The scope of the literature is limited to the past 10 years, in order to underline the contemporality of the research topic. The survey is conducted between 20th and 30th of October 2026, in line with the actuality of the studied issues.

2. HUMAN TRAFFICKING AND CYBERSECURITY /MAIN ISSUES/

Although HT and cyberspace were considered different, not related fields until recently, lately they are becoming consistently more involved with one another. Digitalization provides broader and simpler instruments to perform HT simultaneously among numerous people with different personal characteristics and situated in distant territories. If conducted carefully; such activities may remain undetected for a significant period of time and therefore, no adequate measures are undertaken in prevention and opposing.

The application of information technologies in taking advantages of vulnerable individuals has increased dramatically in recent years. Showing and promoting enslaved people online through social media and public forums is simpler and accessible nowadays. Instead of raising awareness, it encourages traffickers to act. Payment processes and movements from one location to another are also eased by the digital technologies (The California State University, 2025). As a result, cyberspace may turn into a flawless surrounding for conducting HT.

Hence, a new term emerged – cyber trafficking. It refers to crime activities towards HT victims for sexual exploitation taken to "cybersex dens" where through cameras and electronic devices their exploitation is filmed and broadcasted. Cyber trafficking necessitates severe and timely introduced limitations such as law enforcement diligence in investigating cases of cyber trafficking and raising awareness on identifying and communicating HT risks among endangered societal groups (Research Center for Law and Information Technologies, 2022).

Traffickers could apply two types of cyber approaches towards potential victims. The first one is related to actively "hunting" those they believe are more vulnerable and at higher risk of becoming victims. The second one regards passively "fishing" for those who could possibly be misled through posting false ads and waiting for responses to lure them.

Similar to other types of HT, online traffickers might pose as job recruiters advertising non existing career opportunities on social media and job forums (Rhodes, 2017). Scam operators, in contrast to other trafficking organizations, target educated and qualified victims who possess exploitable expertise – language competences, technical or computer background – offering alluring remuneration. Scammers typically cover the victim's

travel cost, yet once they arrive, they seize their passports and IDs, demanding repayment of their "debt". Starvation, mobility restrictions, physical and sexual abuse are frequently associated with the traffickers' compulsion. Moreover, some female victims are coerced into a sex work or used as models in frauds, aiming at recruiting potential scam victims (Preputnik & Flacks, 2023).

Children are especially vulnerable to HT due to their defenseless nature and lack of experience in detecting HT attempts. According to International Labor Organization 40.3 million people, including children, are exposed to HT annually. When technologies are left unrestricted, the same are used by traffickers as instruments for recruitment and manipulation of victims. Regardless of their race, socioeconomic status or place of residence, children are frequently more vulnerable to being targeted by social media, messaging applications and gaming websites. They are used by predators to gain children's confidence, take advantage of their feelings and lure them in risky circumstances (Terry, 2025).

HT is influenced not only by new technologies and performance approaches but also by social changes and suddenly occurred events affecting public wellbeing. Although cryptocurrency, online romance and other digital frauds have been around for decades, the Covid-19 pandemic caused a shift towards their widespread as a HT instrument. It is due mainly to the lack of alternatives – fewer social interactions, limited options for financial actions and difficulties in fraud detection. People were encouraged and occupied in preserving their health, resulting in unrealized neglection of their safety in cyberspace.

Another important factor is the constant evolvement of the HT practices and traffickers' creativity and approach. The systematic training and application of advanced scamming techniques, where victims were coerced into creating forged identities and participating in various cyber frauds, has been linked to a correlation between cybercrimes and HT (Lazarus et al., 2025). Different stimuli may additionally impact the scammers motivation and affect the negative outcome for HT victims.

3. HUMAN TRAFFICKING AND CYBERSECURITY /CURRENT ACTIONS/

Similar to countless other crimes, HT needs to be adequately addressed with appropriate actions in order to mitigate its negative effect. Cybersecurity might turn into an active instrument in that process. The existing actions are supposed to be regularly evaluated, and later on preserved or altered when outdated or inefficient. That provides an opportunity for introduction of new approaches and actions.

In general terms, the process of combating HT is addressed on four main levels:

- ***Prevention*** – warning people about risks of HT, scamming techniques, false job opportunities attracting them abroad, especially when it comes to tech-related employment with suspiciously high remuneration;
- Protection – setting a non-punishment principle for victims in regards to crimes committed as a result of HT and them being forced to perform illegal acts;
- Obstruct scammers – this approach is based on the assumption that HT cases will decline if internet frauds are prevented and the criminal organizations that profit from them are dismantled;
- Fighting corruption – overcoming corruption among government bodies and law enforcement officials has a substantial effect in opposing to HT since they are the responsible authorities for preventing, protecting, and obstructing HT (Preputnik & Flacks, 2023).

The legal legislation regarding HT has a significant focus in protecting people and limiting this crime. The Council of Europe Convention on Action against Trafficking in Human Beings has a broad applicability, including all types of HT towards men, women, and children. The convention's human rights approach and emphasis on victims' protection are its primary added value towards preserving human dignity (Council of Europe, 2025b).

The United Nations General Assembly established Inter-Agency Coordination Group against Trafficking in Persons. It serves as a policy forum to enhance coordination and synergy between United Nations agencies and other related international organizations. The main role of the Agency is to support a comprehensive and all-encompassing strategy for preventing and fighting HT, which includes protection and assistance for HT victims (The Inter-Agency Coordination Group against Trafficking in Persons, 2026).

The primary European Union (EU) legal instrument for combating and safeguarding victims of HT is the EU Anti-Trafficking Directive from 2011, amended in 2024. By defining basic standards for the characterization of criminal offenses and penalties, the Directive lays up a thorough framework for combating HT. Applying a victim-centered approach also incorporates common measures to improve prevention, protection, and victims' support (EUR-Lex, Access to European Union Law, 2024).

The U.S. Trafficking Victims Protection Reauthorization Act of 2023 addresses zones and situations when individuals are most vulnerable to HT. In that manner, it is establishing emergency response procedures. Additionally, the Act improves cooperation between state and municipal law enforcement and implements steps to avoid child marriages (American Bar Association, 2025).

An increasing number of international organizations are concerned with the HT threats and focus their efforts in combating them. The United Nations, Office on Drugs and Crime (2022) (UNODC) as such organization, provides protection guidelines against online HT:

- Establish stern and adequate privacy settings;
- Be cautious with abnormal friend's requests and online contact with presumed acquaintances;

- Refrain from oversharing personal information and sensitive data;
- Stay vigilant and critically assess online invitations that promise unrealistic benefits or unusually high compensation;
- Report everything you consider inappropriate or a security red flag;
- Stay aware of the warning signs of online HT;
- Actively seek assistance in case you are suspecting of being targeted by a trafficker;
- Raise awareness among vulnerable people and share your experience with them (United Nations, Office on Drugs and Crime, 2022).

To combat the growing tendency of HT enabled by contemporary technology, social media and digital platforms, an innovative security operation was carried out in 2024. It was performed under the INTERPOL supervision and with the assistance from Europol, META, STOP THE TRAFFIK, and UNODC. The initiative's participating countries were Brazil, Venezuela, Colombia, Dominic Republic, United Kingdom, Spain, Germany, Ireland and Netherlands. It was funded by the Co-operation in Europe and Global Affairs Canada. A new concerning trend prompted the project – people being trafficked from Latin America after being lured by a misleading job promises, then send to another country, often in Europe, where they are exploited, usually through prostitution. Among the substantial operation's findings are outlined the following: 68 potential victims; 146 possible HT exploiters and recruiters; 365 usernames; and 162 URLs connected to suspicious and questionable activities (INTERPOL, 2024).

The cybersecurity team at ENSCO is dedicated to apply open-source intelligence to facilitate the identification and rescuing of missing and exploited individuals in the escalating battle against HT. Firstly, the crew is trained to distinguish signs of HT and tracking down missing individuals. Afterwards, they are assigned to apply the technology in live operations with real cases of trafficked human beings (ENSCO, 2024).

The main goal of the Convention of Cybersecurity (so called Budapest Convention) is to prevent actions towards deterring of accessibility, integrity, and privacy of computer systems and networks. That is achieved through adoption of adequate measures to effectively combat criminal activities aiming at negatively affecting the computer systems' integrity. For instance, timely detecting, investigating, and prosecuting such actions, establishing arrangements for prompt and inter-dependable international cooperation (Council of Europe, 2026).

In 2022 the Parties to the Budapest Convention were provided with a Second Additional Protocol to the Convention to sign it. It aimed at enhancing collaboration on cybercrime and criminal justice authorities' capacity to obtain electronic evidence for certain criminal investigations or prosecutions (European Union Agency for Criminal Justice Cooperation, 2024). The Council of Europe Group of Experts on Action against Trafficking in Human Beings is in charge of monitoring the execution of the EU Convention (Council of Europe, 2026).

4. SURVEY RESULTS AND ANALYSIS

The conducted survey consists of a questionnaire, divided in four key sections, aiming at providing insights into the discussed topic:

- Description of the questionnaire's role and main goal;
- General information about the respondents – gender and age;
- Evaluation of HT risk – threat level on global scale; threat level on national level (Republic of Bulgaria); threat level on online space; shared personal experience of online targeting;
- HT awareness – evaluation of the level of awareness regarding HT; effective channels for raising awareness; personal actions in HT protection.

The survey consists of 11 questions, combining short, multiple choice, and scale answers. The survey is distributed electronically through an email and shared link among different groups of interested individuals. It is anonymous, personal data is not required, therefor not collected. The survey consists of both required and optional questions. The detailed analysis is presented as follows:

4.1 Respondents' General Information

The total number of respondents in the survey is 84. The questionnaire begins with a gender distribution, outlining the females as a vast majority of all people (65.5%), although the survey was equally distributed to both genders (Figure 1). Historically women are considered more endangered by HT and are generality more vulnerable to online targeting. That might explain men's lower interest in the survey and women's higher involvement in it. However, both groups are providing data, beneficial for the results' analysis and consequent discussion.

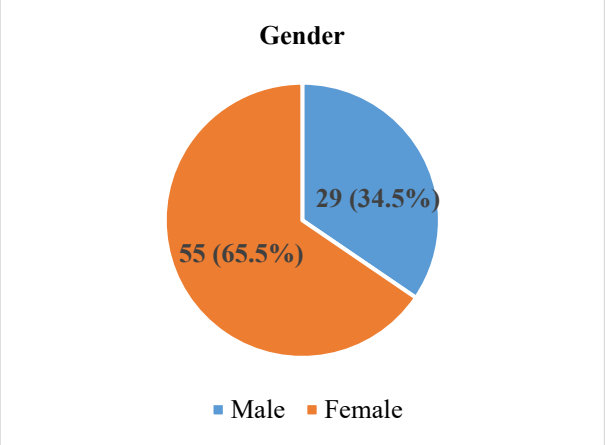

Figure 1. Gender distribution

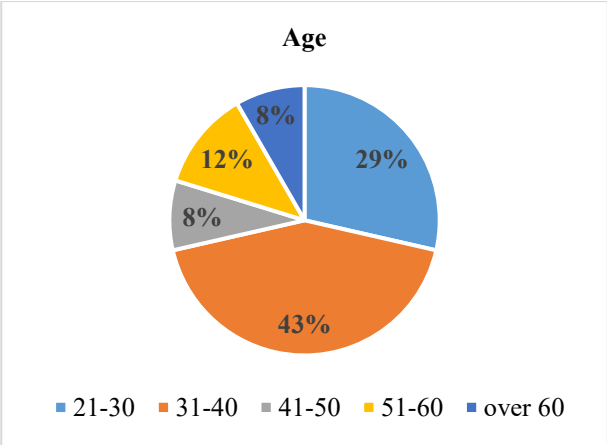

Figure 2. Age distribution

Most of the respondents are between 31 and 40 years old (42.9%), followed by those between 21 and 30 years old (28.6%). Least answers are submitted by the groups of 41-50 years old people (8.3%) and over 60 (8.3%). The distribution is illustrated in Figure 2. The predominantly young demographic in the survey is considered as a valuable source of data regarding young people's opinion on the topic. Nevertheless, the survey is not excluding answers to neither age group, objectively analyzing the received results.

4.2 Evaluation of HT risk

Primarily, respondents are asked to evaluate the level of HT threat in global terms. Secondly, the survey requests to evaluate the level of HT threat specifically in Bulgaria. Answers are presented on a 5-scale (where 1 is "very low" and 5 is "very high"). The comparison (on Figure 3) indicates divergence in people's opinion on global and national display of HT.

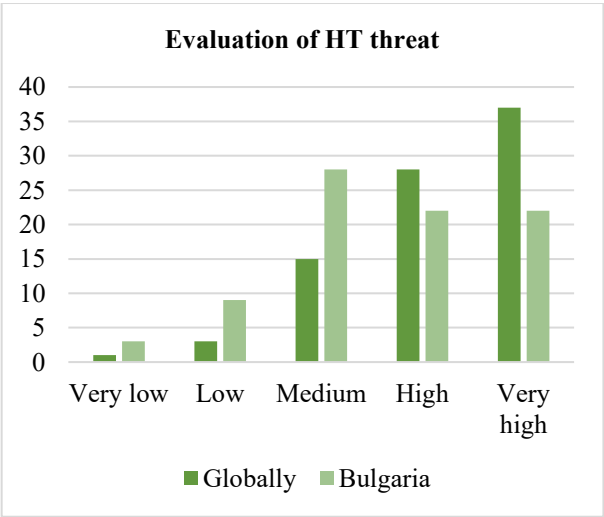

Figure 3. Evaluation of HT threat levels globally and in Bulgaria

Respondents evaluate the global HT threat as medium to very high, yet on national level they consider it slightly lower. Of all surveyed people, 44% state HT threat on global level as "very high", when the percentage regarding HT threat in Bulgaria is significantly reduced – 26%. Instead, most of the respondents (33%) mark "medium" as their perception of HT threat in the country. Around 14% answer "very low" or "low" concerning Bulgaria, opposing to only 5% "very low" or "low" assessment of global level of threat. The average evaluation of HT in global terms is 4.15, while in Bulgaria it is 3.61. That 0.54 variance, once more, highlights the difference in the perception of HT threat levels.

Gender distribution of all participants shows that men consider HT threat in Bulgaria as lower in comparison to women (Figure 4). Since "medium" is the most stated answer in evaluating HT threat in Bulgaria, additional analysis is made, indicating that more than half of the respondents are between 31 and 40 years old, followed by those between 21 and 30 years old (Figure 5). As before, that emphasizes on current young people's perception of medium HT threat on national level.

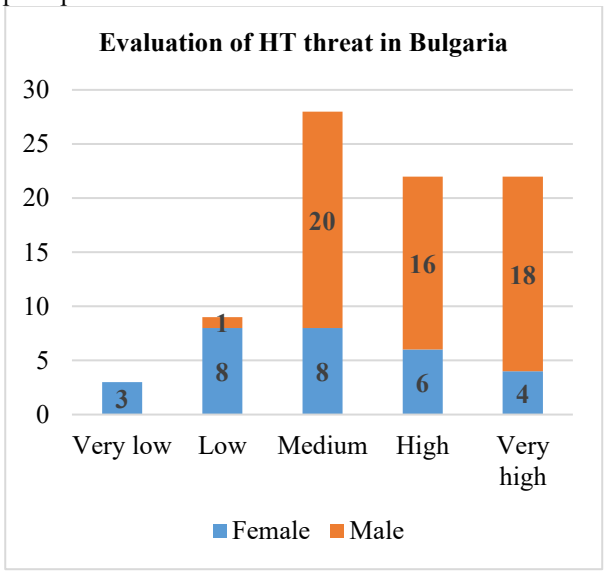

Figure 4. Evaluation of HT threat in Bulgaria based on gender distribution

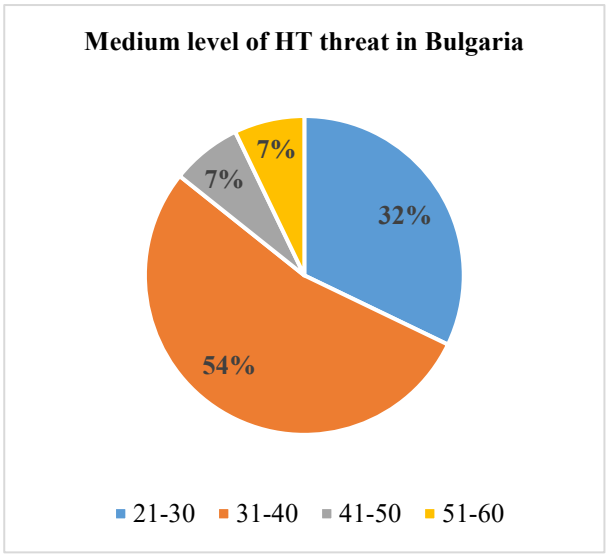

Figure 5. Age distribution of respondents evaluating HT threat in Bulgaria as medium

Afterwards, people are asked to evaluate to what extend online activities increase the risk of HT (Figure 6). Similarly, to the previous questions, the answer options are presented on a 5-scale (where 1 is "very low" and 5 is "very high"). More than half of the respondents (55%) mark "very high", followed by "high" (31%). No one states that the risk is "very low" and only 6% chooses "low", highlighting people's understanding of HT risk while being online. Among those participants who are considering online activities as a factor which increases HT risk, 39% are between 31 and 40 years old, and 30% are between 21 and 30 years old (Figure 7). Other age groups have smaller representatives and yet, they are noticeable. The results in age distribution of this question could be led by the generally higher number of surveyed people in ages between 31-40 years old and 21-30 years old.

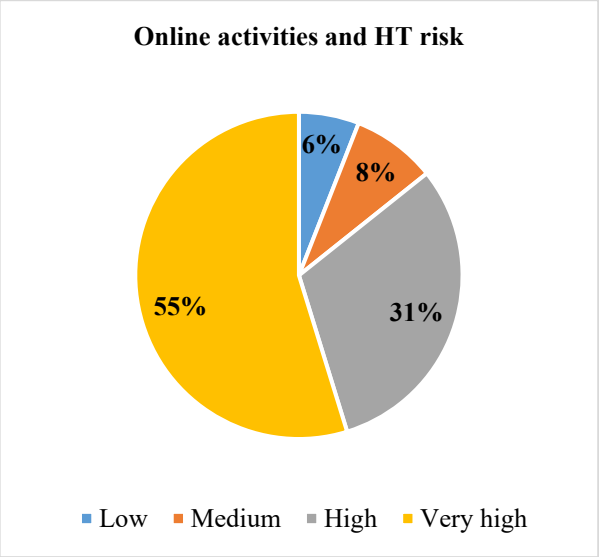

Figure 6. Evaluation of HT risk while online

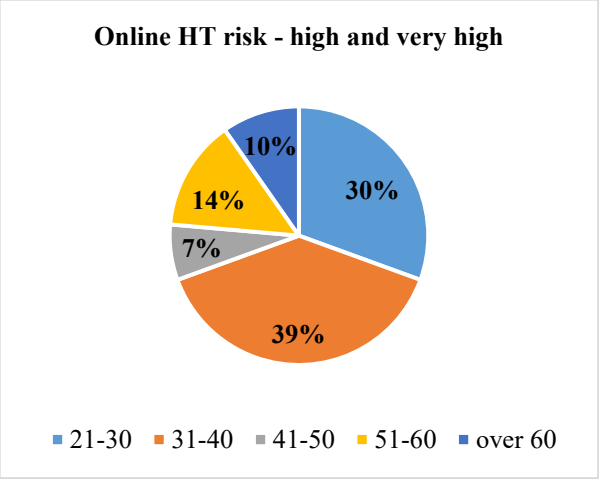

Figure 7. Age distribution of respondents evaluating HT risk while online as high and very high

Next question aims at analyzing whether surveyed people have been victims to HT targeting online (Figure 8). The results are optimistic – 45% of the respondents state they have never been targeted online and 44% choose „most likely not". Yet, 11% (9 people) mark "rather yes". No one answers with "yes". In all three answers female responses are dominant as a major surveyed group. It makes impression that almost all submitted responses "most likely yes" are made by women.

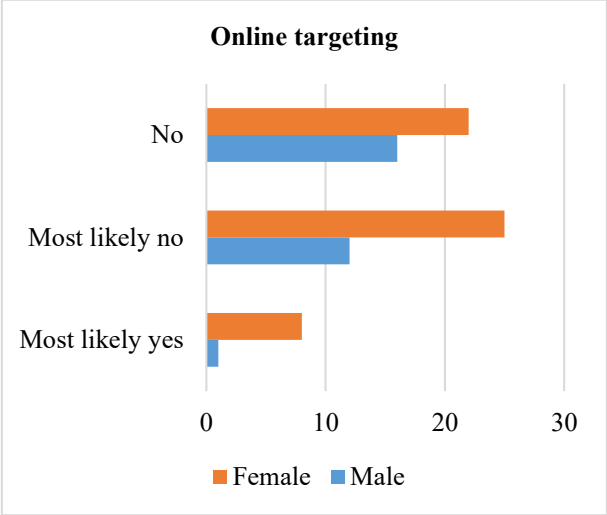

Figure 8. Gender distribution on online HT targeting

At the end of the section people are asked to share what made them suspicious they are being targeted. The question is optional since its delicate matter and only four respondents share their experience:

- Strange and suspicious job offers;
- Asking too many private questions during online communication while not presenting any personal information in return;
- Hidden identity in social media – no name, profile photo or personal details;
- Strangers looking for a friendship through online chat.

4.3 HT awareness

Awareness is considered as a great pillar in safety and fight against HT.

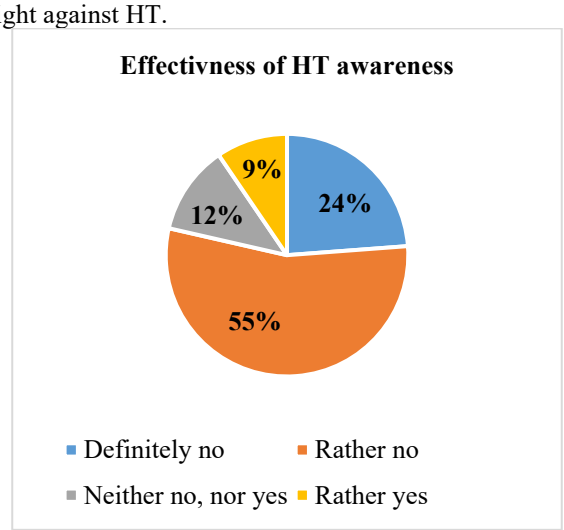

Figure 9. Effectiveness of HT awareness

This section of the survey is dedicated in analysing whether people are conscious about HT and aware how to proceed in order to protect themselves.

When asked about raising awareness (Figure 9), more than half of the respondents consider HT awareness as "rather inefficient" (55.3%). Another 23.5% assess it as "definitely ineffective". That opinion is mostly confirmed by those between 31 and 40 years old and 21 and 30 years old (Figure 10). Less than 10% reflect on HT awareness as "rather effective" and not a single person states it as a "definitely effective".

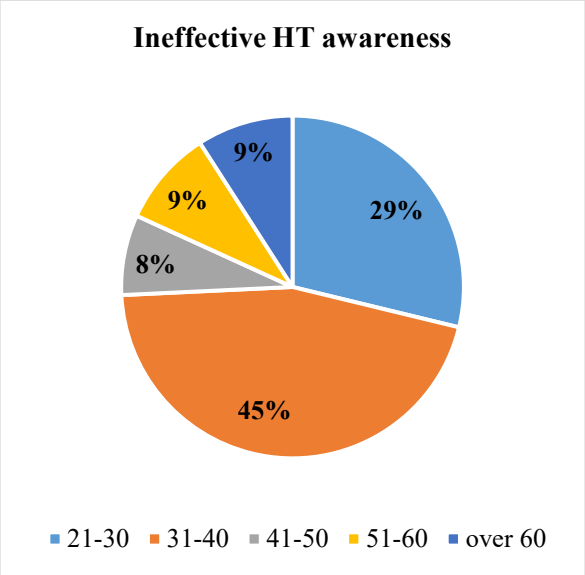

Figure 10. Age distribution of respondents evaluating HT awareness as ineffective

Respondents are asked to point out up to two information channels for raising awareness towards HT threat preferred by them (Figure 11).

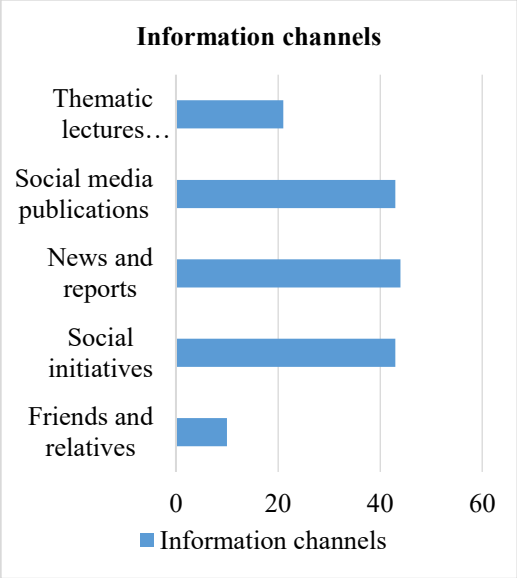

Figure 11. Preferred information channels for raising awareness towards HT

Mostly stated are "news and reports", "social media publications" and "social initiatives". Least preferred option is communication with "friends and relatives". "Thematic lectures and trainings" are also popular, though not a favoured answer. Since the participated individuals in the survey are mainly young people, these results are kind of logical and expected in terms of more social and digitalized point of view of the young generation and information technology development in general.

Next question (Figure 12) aims at analysing whether people apply protection methods against HT through online safety techniques. Almost half of them is actively using safety methods. On the contrary, more than 25% of them are not undertaking any protection approaches. Another 25% state "neither no, nor yes", indicating a hesitation whether they are applying method in any way or whether they are appropriate and HT protection oriented.

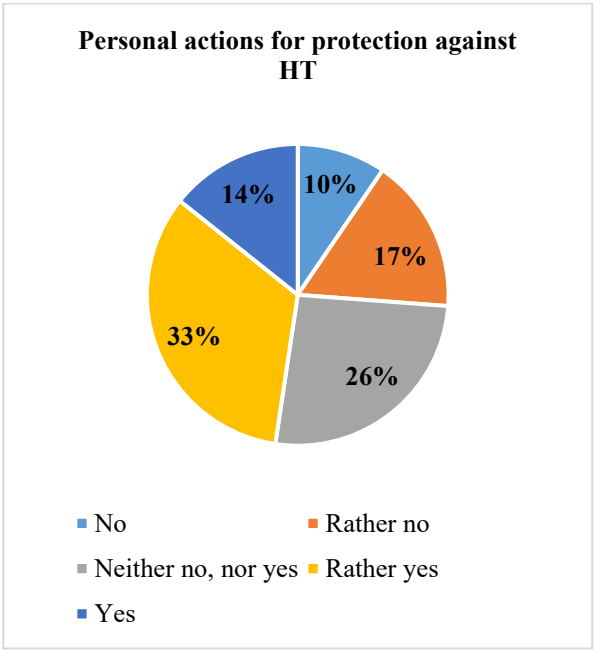

Figure 12. Application of protection methods against HT

Finally, respondents are urged to share what methods they apply to maintain online safety and protection against HT. The most commonly stated answers are related to:

- Be vigilant with contacts online, do not communicate with unfamiliar people and stay alert when being contacted by suspicious individuals;
- Do not share personal information (particularly to strangers), photos (especially of children) and current locations;
- Limit online presence in social media and restrict strangers;
- Report and block suspicious profiles or content;
- Never answer to suspicious or strange emails, nor follow links and unclear sources.

Some of the other answers make an impression as protection approaches, which though helpful for basic online safety, are not quite appropriate and sufficient for fighting HT. As an example, might be listed:

- Do not open unknown or suspicious websites and advertisements;
- Critical thinking towards online sources of information;
- Additional check of information credibility;
- Two-factor identification and regular change of passwords;
- Blocking of spam emails and letters; etc.

Few respondents mention as a prevention technique the installation and application of GPS trackers to locate family members, incl. children, which is also debatable whether could be credited in the group of protection approaches against HT.

5. DISCUSSION

Survey results are leading to several intriguing conclusions requiring discussion and additional study in order to examine future development of the topic, progress in fighting HT, and confirmation or rejection of this line of HT understanding among people.

Firstly, the discrepancy between participants' evaluation of HT risk on global and national level. Although, the difference is not significant, yet people's perception of lower HT threat in Bulgaria is apparent. The variance could be explained by an inability to evaluate the threat level, choosing "medium" as the most optimal average option. In parallel to that, later in the survey more than half of the participants, point out the current HT awareness as ineffective. That might be another explanation for the different evaluation – lack of significant data and proper information regarding HT issues. Gender discrepancies are observed during the whole survey, which might also explain the gender variation here – men tend to consider HT as a lower threat in Bulgaria and medium to high in global terms, in contrast to the women, which are mainly positioning their answers between medium and very high to both global and national levels.

Secondly, low level of online targeting. From the one side, this result is optimistic. On the other side, there is one serious matter to be considered – is there a possibility that respondents fail to identify online targeting even if they are victims of it? Since people stated lower HT awareness in the country, there might be a difficulty in recognizing targeting and react adequately towards it, leaving people with the impression they have never been online targeted.

To sum both results, respondents do not evaluate the risk as high and state themselves as not an online targeting victim and yet, they do not feel abundantly aware of the HT issues, making them even more vulnerable in the future. Inevitably, that might made them biased or not equipped to objectively assess the HT threat.

Thirdly, in line to the above-mentioned conclusions, a quarter of all respondents are not applying any kind of online protection methods to prevent HT towards them. The question arising is: Why? Do they not consider it as a necessary safety instrument? Are they not aware how to approach it and what should do to stay protected? Are they experiencing apathy in HT protection? Understatement and lack of knowledge could pose as an obstacle in people's protection, eventually leading to a higher personal risk, which quite often stay unrealized and unmanaged.

Furthermore, individuals who are applying protection approaches are later sharing techniques which are not quite appropriate and therefor effective in HT protection. Their understanding of online safety is ambiguous, urging them to concentrate on profile protection and digital hygiene, believing that is enough of an effort for all kind of cyber threats, including HT itself.

As a conclusion, lack of awareness hinders the understanding of HT, evaluation of risk and application of protection techniques. Therefore, the main prevention approach towards HT should be related to an adequate and time-related awareness (in that manner – suggested actions, channels of information and reporting mechanisms).

6. RECOMMENDATION FOR FUTURE ENHANCEMENT OF HUMAN TRAFFICKING PREVENTION

In an effort to fight HT, protection mechanisms are required, preferably with a proactive and prevention approach. In its essence the security model regarding HT consists of four main sections (illustrated at Figure 13):

HT as an organized crime and initial element of the model. It is highly influenced by numerous factors, most commonly lack or weakness in security and safety, and victims' vulnerability (due to both low HT awareness and susceptibility of the targeted groups).

Protection actions as a first layer of safety mechanisms. In order to establish an adequate protection policy and appropriate instruments, efforts should be accordingly allocated towards the main HT threats. Strengthened law enforcement and raising awareness are among the basic mechanisms in fighting HT.

Cybersecurity as a second layer of protection. It is a diverse system with unique problem-solving attitude which enables its inclusion in combating HT. Cybersecurity could be of assistance through digital investigations, established professional cybercrime units, cyber intelligence services, AI-support and early detection analysis.

Governance as a final element of the model, "product" of all previous protection mechanisms. It consists of security governance and security strategy, which are interconnected and constantly developing. One could not exist without the other. If security governance is negatively affected, this will inevitably result in a negative effect in the security strategy.

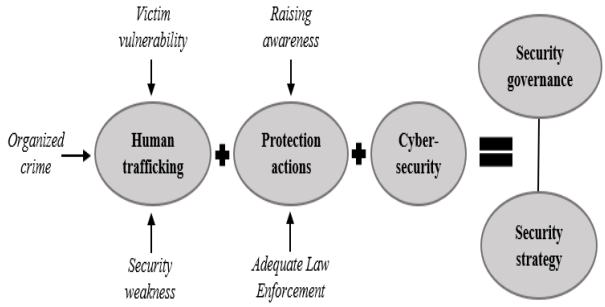

Figure 13. Security Model for Combating HT

Based on the conducted research and survey numerous interrelated recommendations in combating HT are proposed, categorized in the following areas:

- *Establishing an integrated security governance* – as previously stated it aimed at developing a common model for fighting HT. It is essential in forming security strategy and national policy in combating HT;
- *Introduction of sufficient law enforcement* – inadequate legal instruments, large data volumes, data encryption, deficiency in technical equipment and expertise are among the main technological obstacles that affect the investigation of HT cases. That emphasizes on the necessity of funding law enforcement personnel's capacity building in the areas of cyber patrols, internet surveillance, undercover online investigations, social network analysis, and automated search engines for evidence processing (Council of Europe, 2025a);
- *Trainings for identifying HT and prevention* – that process should be aimed not only towards vulnerable groups but also to those related to HT combating, but also to all individuals, especially in most endangered professional areas, social groups and geographic regions. The process could involve cyber intelligence for early warning mechanisms and predictive analysis;
- *Raising awareness through information and social campaigns* – the more discussable HT issues are, the more recognizable they will become. As the survey shows, effective awareness towards HT is a necessity which individuals themselves indicate as an important, however currently, insufficient. Information campaigns through social media, for instance, might be exceptionally effective especially among young people, who spend much of their free time online and massively prefer it as a channel of information. Distributing leaflets, brochures and short video messages could also have a positive effect in raising awareness through bigger number of individuals, as well as news reports and appropriate social initiatives to attract attention;
- *Development of platforms for reporting* – that would not only lead to establishing a database, but also enabling the investigation process and implying punishments for the involved criminals. From a psychological point of view, database is turning HT into a more distinct issue, yet with a reporting focus and investigation attention;
- *Support and professional help for victims* – lack of support might discourage victims to report traffickers and share their experience, unintentionally hindering the crime activity. Their mental state might cloud their judgement and negative reflect on HT investigation and subsequent protection. That necessitates the introduction of support mechanisms and professional help approach;
- *Creating a register (statistics)* – collection of accurate statistical data is shifting HT into a noticeable societal issue, leading to a higher engagement and further involvement of the authority bodies. The creation of a register and regularly updated statistical data may be applied in developing an effective international information sharing, aimed at improving cooperation and common fight of HT;
- *Establishment of new organizations (incl. NGOs)* – although government approach towards HT is more appropriate for combating the crime on a bigger scale, NGOs and other involved domestic and regional organizations could effectively facilitate the process. Special funds, assigned specifically to fight HT, provide adequate subsidizing for raising awareness through information campaigns, trainings, and professional support;
- *Involvement of AI in the process* – since AI is used by many, it could be applied for identification of traffickers or scamming schemes in real time (Triplett, 2024). AI could quickly scan cyberspace regarding suspicious individuals, other submitted signals against them or general scamming practices. It might also provide tips for actions, as well as channels for communication and reporting. With its improved ability to identify, inspect and prevent financial crimes linked to HT, AI has become a game-changing instrument.;
- *Follow closely new tendencies in performance of HT* – criminals are using cutting-edge technologies to recruit victims and earn illegal revenues from HT, making them even more skillful than before. Hence, keeping up with these quickly changing criminal tactics is essential in order to maintain high safety levels. As an example, could be provided the following protection instruments: introduction of cross-sectoral cooperation; monitoring and detection of suspicious activities; individually-based typologies development; nontraditional intelligence tactics and investigative improvement (Bagnall, 2025).

7. CONCLUSSION

HT and cybersecurity are both contemporary phenomena with an increasingly strong impact on modern society, social wellbeing and human rights protection. If HT is not timely mitigated through appropriate mechanisms, it will turn into an excessive threat, which might eventually affect security on multilevel scope. Studying HT reflects on security science through its social, political and security aspects, turning it into an emerging and more noticeable contemporary issue.

Although HT practices are constantly evolving, quite often online oriented, cyber space and digitalization are of great importance in fighting HT. Cybersecurity is an instrument which significantly facilitate the process for protection and prevention of HT. Future policy efforts should focus on strengthening digital investigations, victim support systems, and international cooperation in cyberspace. Law enforcement system and security institutions are both responsible in combating HT, requiring their full attention and increased future efforts in overcoming it.

Raising awareness of HT issues is a vital component of the fight against it. Individuals are not aware of its magnitude, display and threats. As a result, they unintentionally belittle HT and misjudge risks arising from it (on global and national level). Gender and age distribution among surveyed people shows different perception of HT, requiring additional uniformed approach in effectively raising awareness for combating it.

There are no sufficient qualitative and quantitative researches regarding HT, which hinders its real magnitude and opportunities for fight against it. Additional researches are encouraged in the provision of a supplementary perspective of the issues (already acknowledged and potential ones) and identifying appropriate solutions for prevention and mitigation of their effect.

The longer HT remains inadequately unaddressed, the stronger and more resilient it will become. Therefore, a timely response is crucial not only to combating HT, but also to identifying and rescuing victims.

Acknowledgement:

This article is part of a university project ***"Instruments in Combating Human Trafficking"***, subsidized by the science and research fund of the **University of National and World Economy (UNWE)**, Republic of Bulgaria. The project is dedicated to the prevention of HT and raising awareness of its threat.

References:

American Bar Association. (2025). Human Trafficking Legislation, Federal Legislation. https://www.americanbar.org/groups/human_rights/human-trafficking/trafficking-legislation.

Bagnall, C., (2025). AI's Role in Combating Human Trafficking in the Financial Sector. ACAMS Today. https://www.acamstoday.org/ais-role-in-combating-human-trafficking-in-the-financial-sector.

Council of Europe. (2025a). Convention on Cybercrime. https://www.coe.int/en/web/cybercrime/convention-on-cybercrime.

Council of Europe. (2025b). Online Trafficking in Human Beings. https://www.coe.int/en/web/cyberviolence/trafficking-facilitated-by-ict.

Council of Europe. (2026). GRETA - Group of Experts on Action against Trafficking in Human Beings. https://www.coe.int/en/web/anti-human-trafficking/greta.

ENSCO. (2024). ENSCO's Cybersecurity Team Fights Human Trafficking Supporting the CyberFox OSINT4Good Initiative. https://www.ensco.com/news-media/press-releases/ensco-cybersecurity-team-fights-human-trafficking-supporting-cyberfox.

EUR-Lex, Access to European Union Law. (2024). Directive (EU) 2024/1712 of the European Parliament and of the Council on Preventing and Combating Trafficking in Human Beings and Protecting its Victims. https://eur-lex.europa.eu/eli/dir/2024/1712/oj/eng.

Eurojust, European Union Agency for Criminal Justice Cooperation. (2024). Second Additional Protocol to the Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence. https://www.eurojust.europa.eu/publication/second-additional-protocol-budapest-convention-cybercrime-and-cross-border-access.

INTERPOL. (2024). Inside INTERPOL's Probe into Cyber-Enabled Human Trafficking. https://www.interpol.int/en/News-and-Events/News/2024/ Inside-INTERPOL-s-probe-into-cyber-enabled-human-trafficking.

Kadena, E. & Gupi, M. (2021). Human Factors in Cybersecurity: Risks and Impacts. *Security Science Journal. 2(2)*. 51-64. https://www.securityscience.edu.rs/index.php/journal-security-science/article/view/54.

Lazarus, S., Chiang, M., & Button, M. (2026). Assessing human trafficking and cybercrime intersections through survivor narratives. *Deviant Behavior*, *47*(7), 1252-1DOI: 10.1080/01639625.2025.2470402.

Pajić, N. M. (2023). Human Trafficking as a Threat to Personal Security. *Zbornik radova Pravnog fakulteta Novi Sad. 57(3).* 973-988. https://scindeks.ceon.rs/Article.aspx?artid=0550-21792303973P

Preputnik, L. & Flacks M. (2023). Cyber Scamming as a New Destination for Human Trafficking Victims. Center for Strategic & International Studies. https://www.csis.org/analysis/cyber-scamming-new-destination-human-trafficking-victims.

Research Center for Law and Information Technologies. (2022). Cyber-Trafficking. Law and Internet Foundation. https://www.netlaw.bg/en/a/cyber-trafficking.

Rhodes, L. M. (2017). Human Trafficking as Cybercrime. *AGORA International Journal of Administration, no.2.* 23-29. http://univagora.ro/jour/index.php/aijas.

Smith, C. & Brooks, D. (2013). Chapter 1 – Concept of Security. *Security Science, The Theory and Practice of Security.* 1-22. https://www.sciencedirect.com/science/chapter/monograph/abs/pii/B9780123944368000011.

Stöckl, H., Fabbri, C., Cook, H., Galez-Davis, C., Grant, N., Lo, Y., ... & Zimmerman, C. (2021). Human trafficking and violence: Findings from the largest global dataset of trafficking survivors. *Journal of migration and health*, *4*, 100073. DOI: 10.1016/j.jmh.2021.100073.

Terry, K. (2025). The Hidden Threat: Technology and Human Trafficking. Indiana Cybersecurity Hub. https://www.in.gov/cybersecurity/blog/post/the-hidden-threat-technology-and-human-trafficking.

The California State University. (2025). Cybersecurity Fights Human Trafficking. https://www.calstate.edu:443/csu-system/news/Pages/cybersecurity-fights-human-trafficking.aspx.

The Inter-Agency Coordination Group against Trafficking in Persons. (2026). Recommendations on Addressing the Links Between Trafficking in Persons and other Serious Crimes. https://icat.un.org.

Triplett, W. J. (2024). Artificial Intelligence, Cybersecurity, and Human Trafficking Networks. *Cybersecurity and Innovative Technology Journal 2. (2).* 120-125. doi.org/10.53889/citj.v2i2.556.

United Nations, Office on Drugs and Crime. (2022). Technology and Human Trafficking: Avoid the Trap! https://www.unodc.org/unodc/en/endht/2022/internet-safety-tips.html.

Tiana Kaleeva
Affilaition: Postdoctoral researcher
Country: Bulgaria
tianakaleeva@gmail.com
ORCID: 0000-0002-4472-2959