EXTREMIST THREATS ON THE INTERNET AND METHODS OF FIGHTING THEM

Hayitova Hilola Muhammad kizi
Bukhara Region Internal Affairs Department
employee, captain

https://doi.org/10.5281/zenodo.10212559

Abstract: The article describes comments about the Internet becoming a part of the human lifestyle, its use, extremist threats on the Internet, methods and means of combating it, and their practical application.

Key words: Internet, extremism, threat, counter-struggle, social network, NLP

Annotatsiya: Maqolada internetning insoniyat turmush tarzining bir qismiga aylanishi, undan foydalanish, internet tarmog’idagi ekstremistik tahdidlar haqida mulohazalar bayon qilingan bo’lib, unga qarshi kurash usul va vositalari hamda ularni amaliyotda qo’llash haqida so’z yuritilgan.

Kalit so’zlar: Internet, ekstremizm, tahdid, qarshi kurash, ijtimoiy tarmoq, NLP

Аннотация: В статье описаны комментарии о том, как Интернет становится частью образа жизни человека, его использование, экстремистские угрозы в Интернете, методы и средства борьбы с ним, а также их практическое применение.

Ключевые слова: Интернет, экстремизм, угроза, контрборьба, социальная сеть, НЛП.

Today, information and communication technologies and the Internet have entered the lives of most people on earth and have become part of the human way of life. At the moment, more than 8 billion people live on earth [1], 74 percent of them, in other words, 5.3 billion people are Internet users [2].

The Internet is a global computer system connecting large (global) and small (local) computer networks. In it, regardless of geographical location, time and space, some computers and small networks form a global information infrastructure in mutual cooperation. All derivative networks managed by a system of records work together to allow consumers to store, publish, send, receive, search, and exchange information in all known formats (text, sound, video, photo, graphics, music, and other forms).

“The Internet (Latin: inter - aro and net - network) is a worldwide and publicly accessible set of computer networks that exchange information through the standard minimum Internet protocol (I)”[3].

Due to the fact that the Internet does not have a real scale, its boundaries are not clearly reflected as in the real world, and there is a sufficient environment for anonymity, it is natural that it is used as a weapon or tool for social threats. In this article, we will focus on the same aspect, not forgetting that the Internet, along with many useful opportunities, can also be used as a negative tool.

Countering extremist threats online is a complex and important issue. Threats can manifest in various ways, including hate speech, incitement to violence, radicalization, and spreading extremist ideologies. There are some key points to consider when solving this problem.

Monitoring and recording. It is important to monitor the presence of extremist content on social media platforms and other online forums. This may include identifying and reporting content that promotes violence or hate. However, balancing this with freedom of expression and privacy is a critical issue.

Monitoring and recording extremist content on the Internet involves several methods and strategies, each with unique challenges and advantages. Below we will touch on some of these methods and technologies;

1. Automated detection tools: Many social media platforms and websites use automated systems to identify extremist content. These tools often rely on algorithms and machine learning to scan for specific keywords, phrases or patterns that indicate extremist material. Despite being effective at processing large volumes of data, they are not always able to distinguish clearly between malicious content and legitimate free speech, but are highly effective. Below are examples of automated detection tools and the technologies they use:

a) content-matching algorithms: These tools use algorithms to match online content to a database of known extremist material. For example, Facebook's "hashing" technology creates digital fingerprints of banned content, allowing the platform to identify and remove the same or similar content shared elsewhere on the site.

b) machine learning and artificial intelligence algorithms: Advanced machine learning models are trained to recognize patterns that indicate extremist content, such as specific phrases, characters, or patterns of behavior. These models can learn and adapt over time, improving their accuracy. For example, Google's Jigsaw project uses machine learning to detect malicious content online.

c) Natural Language Processing (NLP): NLP technologies enable automated analysis of text content for signs of extremist rhetoric. These tools can understand context and nuances in language, which can be critical in distinguishing between malicious content and legitimate discussion.

d) image and video recognition technology: With the proliferation of multimedia content, automated tools that can analyze images and videos are becoming important. These tools use pattern recognition and other SI techniques to identify extremist symbols, propaganda, or images of violence in visual content.

e) network analysis tools: These tools analyze social interactions and communication patterns on platforms to identify networks of extremist users or groups. By understanding these networks, platforms can more effectively target content that violates their policies.

f) behavioral analysis systems: Some tools focus on user behavior, such as the frequency of posting certain types of content, interaction patterns, or the rapid spread of specific messages. These metrics help identify accounts that promote extremist ideologies.

g) Sentiment Analysis Tools: Sentiment analysis is used to determine the tone and intent behind posts, which can be useful in identifying content that promotes hate or violence, even if it does not use explicitly prohibited words or phrases.

These automated detection tools are important in the fight against online extremism, but they are not completely reliable. They should be supplemented with human oversight to ensure accuracy and handle sensitive situations where context matters. In addition, when using these technologies, as we noted above, it is necessary to always pay attention to aspects related to privacy and freedom of speech.

2. User reporting systems: Platforms often encourage users to report extremist content. This method relies on the vigilance of the platform community. User reports are usually reviewed by moderators, who decide whether the content violates the platform's policies. This approach can be effective, but relies on user participation and moderator input.

3. Special monitoring groups: Some organizations and governments set up special teams to monitor online spaces for extremist content. These teams may consist of analysts, linguists and experts on extremist ideologies. They manually scan websites, forums and social media platforms for signs of extremist activity.

4. Cooperation with law enforcement and intelligence agencies: Platforms may cooperate with law enforcement and intelligence agencies to identify and monitor extremist content. This could include sharing information and leveraging the expertise of these agencies to better understand the nature of the threat.

5. Third Party Monitoring Services: There are third-party organizations that specialize in online extremism monitoring. These organizations work independently or in partnership with platforms and governments to identify and report extremist content. They often have special knowledge and tools to help with monitoring.

6. Community engagement and involvement: Cooperation with communities affected by extremism can be an important monitoring tool. Community members can provide insight or report online activities that may not be apparent to outside observers.

7. Cross-platform analysis: Extremists often operate on multiple platforms. Effective monitoring involves analyzing content and activity on various social media, forums, and websites to understand broader patterns and networks.

8. Data analysis and research: Analyzing data trends, such as spikes in certain search terms or sharing patterns of certain posts, can help identify emerging extremist trends or campaigns.

Effective online monitoring and reporting of extremist content requires a combination of these methods. Continually adapting and refining these strategies is important, as extremist groups often change their tactics to avoid detection. In addition, respecting the rights to privacy and free speech when using these methods is essential to maintaining the trust and cooperation of the online community.

Cooperation with technical companies. Governments and law enforcement agencies often work with technology companies to identify and remove extremist content. This collaboration may also include the development of algorithms and tools to proactively identify such content.

Counter messages. Developing and promoting counter-narratives is essential in the fight against extremist ideologies. This involves creating content that challenges extremist views and offers alternative perspectives, often aimed at vulnerable individuals who may be vulnerable to radicalisation.

Education and awareness. Educating the public, especially young people, about the dangers of extremism online is critical. This can include teaching critical thinking skills, digital literacy and the ability to recognize and counter extremist propaganda.

Legal grounds. Implementation and enforcement of laws specifically addressing online extremism is critical. This includes laws against hate speech, incitement to violence and distribution of terrorist material.

International cooperation. Extremist threats often cross borders, making international cooperation essential. Sharing intelligence, best practices and strategies between countries can be effective in combating online extremism.

Support for affected communities. Support for communities and individuals targeted by online extremism, including counseling and safety measures, is critical to both prevention and response.

Respect for human rights. Any measures taken to combat online extremism must respect human rights and civil liberties. This includes ensuring that actions against such content are lawful, necessary and proportionate.

Countering online extremism requires a multi-pronged approach that combines technology, education, legal measures and international cooperation. It is a delicate balance between preserving freedom of expression and ensuring that online spaces are not used to promote violence and hatred.

References:

1. https://www.worldometers.info/world-population/
2. https://www.statista.com/statistics/617136/digital-population-worldwide/
3. https://uz.wikipedia.org/wiki/Internet
4. Sharofovich S. A. Virtualization of economy is the main mechanism of virtualization of social life //American Journal Of Social Sciences And Humanity Research. – 2022. – T. 2. – №. 12. – C. 62-68.
5. Sharofovich S. A. Virtuality as a New Ontological Model of the World //Central Asian Journal of Literature, Philosophy and Culture. – 2021. – T. 2. – №. 10. – C. 51-54.