Check for updates

DOI: https://doi.org/10.34069/AI/2024.82.10.8

How to Cite:
Nikitenko, L., Sharmar, O., Marusiak, O., Honcharuk, V., & Yanivskyi, V. (2024). Social media as an emerging threat to national security. *Amazonia Investiga, 13*(82), 100-111. https://doi.org/10.34069/AI/2024.82.10.8

Social media as an emerging threat to national security

Соціальні мережі як нова загроза національній безпеці

Received: September 1, 2024 Accepted: October 28, 2024

Written by:
Lilia Nikitenko[1]
https://orcid.org/0000-0002-2152-4255
Olha Sharmar[2]
https://orcid.org/0000-0002-9123-8668
Oleksandr Marusiak[3]
https://orcid.org/0000-0002-4113-0624
Vladyslav Honcharuk[4]
https://orcid.org/0000-0002-9627-9530
Volodymyr Yanivskyi[5]
https://orcid.org/0009-0004-5920-4566

Abstract

This paper explores in depth the growing impact of social media on national security across the globe while highlighting the risks posed by the rapid dissemination of information, the organization of unauthorized protests, and the spread of disinformation. It has been demonstrated that social media platforms such as Facebook, Twitter, Telegram and TikTok have been utilized by various actors, including activists, radical groups, and foreign states, in order to influence public opinion, incite violence, and destabilize governments. A comparative analysis of global events like the Arab Spring, the 2016 U.S. elections, Hamas attack against Israel, and protests in Hong Kong demonstrates how such platforms can serve dual purposes: fostering democratic values while simultaneously being exploited to undermine national stability. The research also

Анотація

У статті поглиблено досліджується зростаючий вплив соціальних мереж на національну безпеку в нашому світі, а також висвітлюються ризики, пов’язані зі швидким поширенням інформації, організацією несанкціонованих протестів та поширенням дезінформації. Продемонстровано, що соціальні медіа-платформи, такі як Facebook, Twitter, Telegram і TikTok використовують різні суб’єкти, включаючи активістів, радикальні групи та іноземні держави, з використанням впливу на громадську думку, підбурювання до насильства та дестабілізації діяльності урядів. Порівняльний аналіз таких глобальних подій, як Арабська весна, вибори в США 2016 року, атака ХАМАС на Ізраїль і протести в Гонконзі, демонструє, як такі платформи можуть служити подвійним цілям: сприяти підвищенню демократичних цінностей і водночас

[1] Candidate of Legal Sciences, Associate Professor of Law, Associate Professor of the Department of Constitutional, International and Criminal Law of the Vasyl Stus Donetsk National University, Ukraine. WoS Researcher ID: LMN-2029-2024 - Email: lilya@donnu.edu.ua

[2] Candidate of Legal Sciences, Associate Professor of Law, Associate Professor of the Department of Criminal Law of the National Academy of Internal Affairs, Ukraine. WoS Researcher ID: LPP-8352-2024

[3] Doctor of Philosophy in Law, Senior Research Fellow of the Scientific Research Institute of State Building and Local Government of the National Academy of Law Sciences of Ukraine, Ukraine. WoS Researcher ID: ACX-5501-2022

[4] Doctor of Philosophy in Law, Associate Professor, Associate professor of the Department of Financial and Economic Security Management, Institute of Security, Interregional Academy of Personnel Management, Ukraine. WoS Researcher ID: LPQ-3758-2024

[5] Postgraduate Student of the Department of Constitutional, International and Criminal Law of the Vasyl Stus Donetsk National University, Ukraine. WoS Researcher ID: LPQ-3066-2024

addresses the specific issue of separatism, where social media is used to disseminate ideologies that threaten territorial integrity and constitutional order. The proposed study also examines the potential of cyberattacks coordinated via social media, thus highlighting the vulnerability of state institutions and critical infrastructure. The research concludes by stressing the urgent need for a balanced regulation of social media, offering insights into international legal frameworks, enhanced cybersecurity measures, and also various challenges in maintaining both freedom of expression and national security.

An elaborated set of research methods (comparative, historical, method of systemic analyses) has been actively used in the course of this research, thus enabling the authors to combine theoretical observations with comprehensive data analyses.

Existing legislative approaches to regulating social media in the context of protecting national security interests in various jurisdictions, including Israel, China, Pakistan, the United States, and Ukraine, have been covered in the paper.

Keywords: national security, information society, criminal liability, social media, communication technologies.

використовуватися для підвищення національної стабільності. У дослідженні також вивчається конкретна проблема сепаратизму, коли соціальні медіа використовують для поширення ідеології, що загрожує територіальній цілісності та конституційному ладу. У пропонованому дослідженні також розглядається потенціал кібератак, скоординованих через соціальні мережі, що підкреслює вразливість державних інституцій та критично важливої інфраструктури. У висновках дослідження підкреслюється нагальна потреба у збалансованому регулюванні соціальних мереж, пропонується розуміння міжнародної правової бази, посилення заходів кібербезпеки, а також різних викликів у підтримці як свободи виразу поглядів, так і національної безпеки.

У процесі виконання цього дослідження активно використовувався розроблений набір методів дослідження (порівняльний, історичний, метод системного аналізу), що дозволило авторам поєднати теоретичні спостереження з комплексним аналізом даних.

У статті висвітлено існуючі законодавчі підходи до регулювання соціальних медіа в контексті захисту інтересів національної безпеки в різних юрисдикціях, зокрема в Ізраїлі, Китаї, Пакистані, США та Україні.

Ключові слова: національна безпека, інформаційне суспільство, кримінальна відповідальність, соціальні медіа, комунікаційні технології.

Introduction

Today, social networks have become popular platforms for spreading public messages and calls for action, which may threaten national security. Here are just a few typical ways that demonstrate how this happens.

First, the rapid dissemination of information, as social media allows for the instantaneous dissemination of information to a large audience of users. This can include both true information and disinformation, which can manipulate public opinion.

Second, it is the organization of protests and actions, including those unauthorized by the governments and obviously dangerous (armed) ones. In particular, social media platforms such as Facebook, Twitter, and Telegram are used to organize mass protests and actions. For example, activists can quickly mobilize a large number of people to participate in protests using Facebook groups and relevant messengers.

Third, the spread of disinformation and fake news, as social media is often used to spread fake news and other messages that can undermine national security by creating panic or distrust of the government on the part of the public. The so-called bots and trolls can actively spread such news, making it difficult to identify their source, a tactic actively used by the aggressor state. It is also worth paying attention to the manipulation of public consciousness, as platforms can be used to manipulate public opinion through targeted advertising and specially designed campaigns that undermine trust in democratic processes, such as elections and public accountability.

Fourth, it can be radicalization and recruitment. Radical groups use social media to recruit new members and spread extremist ideologies. This may include the use of closed groups and channels to discuss and plan joint destructive actions, influence operations, terrorist acts, etc.

Finally, it is the coordination of cyberattacks, as social media can be used to coordinate cyberattacks on state institutions, companies, or critical infrastructure, which can have serious consequences for the national security framework.

This study seeks to analyze the growing influence of social media on national security by examining how digital platforms are used to: spread disinformation and manipulate public opinion; organize unauthorized protests and radicalize individuals; coordinate cyberattacks on state institutions and critical infrastructure; promote separatist ideologies and destabilize territorial integrity; highlight global case studies (e.g., Arab Spring, U.S. elections, Hong Kong protests) to demonstrate the dual-purpose nature of social media as both a democratic tool and a destabilizing force. The research aims to offer a balanced regulatory approach for social media that safeguards national security without stifling key democratic freedoms.

Apart from the abstract and introduction sections, this paper included the following sections:

- Literature review – reviews existing research on the impact of social media on global conflicts, emphasizing its role in separatist movements and disinformation campaigns;
- Methodology – describes the research methods used, including comparative legal, historical, and systemic analyses, to explore social media's influence across various jurisdictions;
- Results and discussion – examines global case studies (e.g., Arab Spring, Russian disinformation campaigns) and the misuse of platforms like Facebook, Telegram, and TikTok. Discusses legal and cybersecurity responses in jurisdictions like the U.S., Ukraine, and China;
- Conclusions - highlights the dual role of social media as a tool for freedom and as a threat to national security while advocating for balanced regulation and international cooperation to address those challenges.

Literature review

Recently, legal commentators have been more actively researching the expanding phenomenon of social media in the context of globalization trends as well as threats to national security in various countries. A few authors and their scholarship are worth mentioning here.

E. Brooking, L. Mashkoor, L., and J. Malaret have jointly researched the impact of social media on the massive ongoing Middle East crises, how terrorists have been communicating, and even soliciting financial donations for their illegal activities through various social media platforms (Brooking et al., 2023).

J. Cox J. And J. Koebler have discussed a number of issues related to white nationalism and white separatism movements on Facebook and also how this powerful media platform has reacted to these threats by issuing content ban orders.

Also, a number of legal commentators from various "conflict zones" jurisdictions have commented on the negative impact on internal politics and public affairs, caused largely by bad actors' manipulations relying on social media pages and challenges. For example, Pakistani scholar A. R. Iqbal has written on the pressing issues of social networking in Pakistan and how it fuels the separatist movement in the province of Balochistan.

In addition to publications on the topic of social media "weaponization" in various academic journals, a number of high-quality articles have also appeared on the pages of the "Amazonia Investiga" multidisciplinary journal. A recent paper on the topic of prosecuting cases of humanitarian aid embezzlement during the war in Ukraine explains how social media plays an important role in committing war-related crimes (Kamensky et al., 2023).

A group of Ukrainian scholars have recently published a paper, which discusses the importance of information security of critical infrastructure objects to guarantee Ukraine's national security (Chernysh at al., 2023). Though not focusing directly on the issues of social media and national security, it explains how access to information and various digital capabilities can have both a positive and negative impact on the national security ecosystem.

At the same time, various Internet platforms can serve for good as alternative sources of information during the period of war, as argued by a group of social communication researchers (Horska et al., 2023).
Overall, the ongoing academic discussion of such topics as an overview of social media in the national security context (Kasi et al., 2021), social media as a potential platform for extremism (Ganesh & Bright, 2020), impacts of social media on national security in various jurisdictions (Chukwuere & Onyebukwa, 2018), even the impact of modern education in the field of national security (Myroshnychenko et al., 2024) has recently intensified. The main reason for this lies primarily in the current global challenges and significant shifts in the global security architecture.

One can safely guess that with the further development of social media and also with the ongoing armed conflicts in various parts of the world, more research efforts by legal, national security, and military scholars will be given to this topic in the future.

Methodology

In the course of working on this paper, the following research methods have been used:

- The comparative legal method was chosen as a key tool of research with the goal of comparing how social networks affect national security interests in various jurisdictions and also how national governments respond to various threats posed by such networks. In particular, this method has been extensively used by Ukrainian scholars in the course of their research (Movchan et al., 2022) due to the fact that the Ukrainian independent legal system is a comparatively new one and foreign expertise in various legal issues is highly welcomed;
- The historical method allowed us to look into the origins of the growing social media phenomenon worldwide and how it has gradually become a real, though digital, threat for the national security and defense frameworks in different countries;
- The method of systemic analyses enabled to take an in-depth look into the globalized nature of modern social networks and also how their interconnectivity and access to billions of customers worldwide can affect national security interests, even more so in the polarized world of today. In modern research, when discussing various globalization-related issues, the method of systemic analyses becomes an important tool for "all-inclusive", multidirectional analyses (Lutsenko et al., 2023).

Results and Discussion

The territorial integrity of nations is often perceived as a prerequisite for a functioning, unifying national identity. However, the economic and technological development of recent decades has enabled experts to question this assumption. It can no longer be taken for granted that people who identify with a given nation live in the same space, nor can it be assumed that cultural homogenization occurs at the national level through the media. In fact, today, nations thrive in cyberspace, and the Internet has become a key technology for "holding" nations (and other abstract communities) together in just a few years. Countries which have lost their territory (such as the Afrikaner-led South Africa), countries that have been disintegrated for political reasons (such as Tamil Sri Lanka or Kurdistan), countries with large temporary foreign diasporas (such as the Scandinavian countries, with their large communities in Spain in winter, or the large presence of Canadians in the US state of Florida, also in winter) or countries where many citizens work temporarily or permanently abroad (e.g. India or Caribbean island states or Ukraine) are represented on many Internet sites, from online newspapers and magazines to semi-official news sites and "virtual communities" home pages. According to many experts, in the current period of globalization and integration, the Internet is used to strengthen rather than weaken national identities (Eriksen, 2007).

Our analysis of the use of social media and various Internet resources to the detriment of national security interests has demonstrated that in most countries where this phenomenon can be traced, we are talking about the phenomenon of separatism, one of which manifestations is the actual use of social media as a kind of platform for calls for violence, terrorist acts, and the actual separation of a certain territory from an existing state recognized by the international community.

It is noteworthy that this refers to public calls against public security in the context of separatism, treason, calls to overthrow the constitutional order or seize state power, or commit other crimes against national security. In the language of the Ukrainian criminal law (Article 110 of the Criminal Code of Ukraine), this includes public calls, through the use of social media, to change the boundaries of the territory or state border in violation of the constitutional or other official order, as well as public calls or distribution of materials calling for such actions (Criminal Code of Ukraine, 2021).

For the purposes of our analyses, as reflected in the title of this paper and without any unnecessary political bias, here are some contemporary examples of social media being used to organize mass protests and other social actions.

1. The Arab Spring (2010-2011): social media played a key role in coordinating and mobilizing protests in many countries of the Middle East and North Africa. Activists used Facebook and Twitter to organize protests and draw the attention of the international community.
2. Russian disinformation campaign during the US elections (2016): Russian agents used social media to spread disinformation and fake news to influence the outcome of the US presidential election.
3. Protests in Hong Kong (2019): social media platforms, primarily Telegram and Twitter, were actively used to organize protests and disseminate information about police actions and the safety of protesters.

Thus, social media can be described as a dual-purpose tool: it can promote democratic values and freedom of speech, but it can also be used to undermine national security and destabilize society. Thus, a balanced approach to their regulation and monitoring by state authorities is required.

As one recent and large-scale example of illegal use of social media resources, in March 2019, Facebook banned white nationalism and white separatism on its platform, which was a major change in the communication policy of the world's largest social network with over 2 billion users. Facebook will also start directing users, who try to post content related to these ideologies to a non-profit organization that helps people leave hate groups. This policy applies to both Facebook and another popular social network, Instagram. Experts note that the social movements of white nationalism and white separatism are different from other separatist movements, such as the Basque separatist movement in France and Spain and black separatist movements around the world, because of the long history of white supremacism which has been used to subjugate and dehumanize people of color in the United States and around the world (Cox & Koebler, 2019).

At the same time, in the context of our study, the above provisions emphasize the growing awareness of the management of the largest social networks about the dangers of certain social movements, groups, and, in particular, those promoting separatism, hatred, violence, and various forms of discrimination.

Moving on with our analysis of modern foreign experience in countering public appeals, we will refer to the relevant Pakistani experience. Abdul Rauf Iqbal, a Pakistani scholar, states that, on the one hand, Internet has become the main open source of information, with social media emerging as an important platform for civil society. In a political discourse, it has created a coordinating tool for almost all political forces in the world. In particular, development of the global network is creating a similarly favorable environment in Balochistan, Pakistan's largest province[6]. For example, the Dissident Balochs group has its own Facebook page, using pseudonyms, real names, and profiles of like-minded activists and sympathizers. They create new Facebook pages, new social media communities, and coordinate joint events. They have a presence on Twitter (currently social network X), where they disseminate information, articles, blogs and videos in support of their ideology and actions. They have daily video content on YouTube channel, their own newsletters, and their own audience both inside and outside of Pakistan.

Having analyzed Facebook pages for empirical data on Balochistan separatists, the author concluded that eighteen out of thirty pages call for the spread of online separatism, while only two pages further the federal

[6] As a reference: Balochistan is a historical region on the northern coast of the Indian Ocean, located on the border of the Middle East and Hindustan regions. It is administratively divided into provinces that are part of the neighboring countries: Afghanistan (Helmand, Kandahar), Iran (Sistan and Baluchistan) and Pakistan (province with the the same name). The main religion in this region is Islam. The Baloch have not abandoned the idea of creating their own independent state. The Baloch of Iran and Afghanistan, as well as the Pashtuns, who number more than 4 million people in the province of Balochistan, are in solidarity with the Baloch of Pakistan. In some areas of the province, guerrillas continue their activities aimed at separating the region, in some cases attacking armed forces units.

ideology of a unified Pakistan. This means that the separatists' online reach and, consequently, audience is much larger than that of the federalists. Although the total number of separatists is only in the thousands, the increase in the number of dissident pages signifies a radical trend in social media, especially in the case of Balochistan. This, the author concludes, is an alarming trend that needs to be seriously studied and potentially addressed (Iqbal, 2011).

Every social movement, whether legitimate or banned, requires financial resources, and the Baloch use their natural resources for economic gain; the province also enjoys external financial support. Because, and this is obvious, the national media is hostile to the Baloch insurgency, they have long used social media to communicate effectively. The ongoing struggle for an independent Balochistan is accompanied by the use of common symbols that characterize the movement. All of this indicates that Islamabad's policy of largely ignoring the province has created a vacuum that the Baloch insurgent leadership is exploiting. It is also worth noting that insurgents' messages and appeals have shifted to social media sites, which are used by billions of users around the world. Internet is a cheaper medium and at the same time it is an extremely fast tool for disseminating information. Hence, the spread of insurgent (separatist) ideology on these sites creates a new wave of social mobilization on the Internet. Although there are relatively few of them at the moment, active use of social media sites can, as experts warn, cause dangerous unrest in the political discourse of Pakistan (Iqbal, 2011).

By the way, in the first months of 2024, attacks and terrorist attacks became more frequent in this huge and resource-rich province. Intense shelling and the use of suicide bombers were directed against Pakistani security forces as well as foreigners. Responsibility for most of the attacks was claimed by the Baloch Liberation Army (until 2022, it had its own Telegram network presence), a separatist militant group that the United States has designated as a terrorist organization (Siddique, 2024).

Moving on in our analysis of countering public appeals in various jurisdictions, we would like to note the following. Experts of the authoritative American research organization "RAND" have concluded, based on the results of a comprehensive analysis, that the social network Twitter has made a coordinated attempt to influence the upcoming presidential election in the United States – with the help of trolls (fake identities that spread political/social narratives) and superconnectors (accounts with high network connections on social platforms) – is aimed at sowing distrust, exacerbating political divisions, and undermining confidence in the foundations of American democracy. While RAND experts acknowledged that they could not definitively attribute the past interference in the presidential election to a specific actor, the tactics and trend they observed on Twitter reflect Russia's longstanding strategy of exploiting existing tensions between the parties to create a sense of disunity among U.S. voters; they also advance Russia's geopolitical interests.

According to W. Marcellino, leading author of the study and a scholar of social issues and behavior at RAND, social media has made it much cheaper and easier for foreign actors to launch increasingly sophisticated attacks on democratic processes and political discourse in any given nation. He adds that many Americans are now immersed in online conversations that have been artificially shaped and that give them a false and distorted picture of the world and events in it. The study used software tools developed by RAND to analyze a large dataset of 2.2 million tweets from 630,391 unique Twitter accounts collected between January 1 and May 6, 2020. The comprehensive analysis revealed that troll and superconnector accounts were predominantly grouped in certain Twitter groups that were involved in political discussions about the presidential election (Marcellino et al., 2020).

Social media has allowed us to communicate more easily and quickly than ever before. At the same time, they have also created a new "platform" with a potential for committing offenses and communicating among offenders. Homeland security, customs and border security, law enforcement, and other organizations can monitor publicly available information on social media to gain threat intelligence – to detect and mitigate criminal activity and potentially stop it in its tracks.

Interpol reports that terrorists are now using social media for "radicalization, recruitment, financing and planning of terrorist activities". As part of its counterterrorism efforts, INTERPOL and other law enforcement agencies are able to track suspected terrorists, examine social media posts, and update suspect lists as necessary. Similarly, visa pre-application officers can use social media threat monitoring to check applicants' online activities to determine whether they are in any way connected to terrorists on watch lists (Marcellino et al., 2020).

Today social media are regularly used to conduct disinformation campaigns of various kinds and intensity. First and foremost, we are talking about disinformation campaigns aimed at undermining national security and constitutional order in a particular state. The use of fake news is an effective tool for organized disinformation campaigns aimed at destabilizing states by undermining foundations of public life and democratic processes, including elections. This category has the most destructive impact on national security and social cohesion in any given state.

Recently, bots have become a part of the social media landscape, at least in the medium term. Innovations in parallel computing and improvements in algorithm construction are expected to make it more difficult to distinguish artificial bots from real users, i.e. humans. Some researchers believe they have discovered fake Facebook groups almost entirely filled with bots. These fake groups, if skillfully managed and organized, could eventually engage real users in certain socio-political processes, such as elections (Vasu et al., 2018).

Currently, U.S. federal law enforcement agencies are very active (in some cases even aggressive) in responding to disinformation (not always calls) on the Internet, including social media.

American journalists and lawyers agree that today media plays an important role in shaping public opinion about national security policy and its legal parameters, and therefore bear a great responsibility for performing the media function with the highest possible degree of professionalism. Since the 9/11 terrorist attacks, many complex and sensitive issues related to national security and the rule of law have arisen, thus increasing the challenge for the media to fulfill their role with care and accuracy. Some of these aspects reflect the inherent tension between the principles of civil liberties, privacy, due process and human rights.

Analyzing some of the problematic issues related to the impact of social media on national security interests, Pakistani authors argue that social media can, on the one hand, pose a threat to national security, and on the other hand, serve as a useful tool or asset for protecting national interests of the state. The authors conclude that terrorist organizations use social media as a tool for ideological radicalization, communication, and training of their members, and thus can threaten security of any state in the world. Researchers also make a reasoned assumption that future revolutions, military conflicts and other social disasters will increasingly take place in societies whose members are connected via media and other information technologies. Social media, as one of the manifestations of hybrid warfare, is already being used by the military in many countries and is likely to become even more active. During a large-scale conflict, the purpose of using social media is to mislead, propagandize and directly influence society (Kasi et al., 2021). Unfortunately, this is currently happening, on a much bigger scale, against the backdrop of the war in Ukraine.

As another researcher aptly puts it, in the era of the information revolution, the media is the most influential tool for persuading national policies and interests. It is becoming clear that governments desperately need the increased support of the media to project their clear position and moral supremacy. An exploratory perusal of the news and headlines convinces us that the print media in Pakistan remains more than patriotic. The time has come for the government to take appropriate measures to improve its own media profile. Failure to recognize and counteract the enemy’s use of the media can lead to unprecedented military and national defeats. Thus, in today’s technologically complicated world, media will continue to remain a tool for the effective realization of national interests (Hussain, 2008).

Next, within the framework of our comparative legal analysis, we will turn to the issue of a potential threat to the US national security from the popular social network TikTok.

Despite the fact that TikTok seeks to distance itself from the official Chinese authorities, China’s current aggressive policy “sheds light” on the possibility of maintaining covert ties between this social network and the Chinese government.

As a matter of national security priorities, the US Department of Defense in its current Cybersecurity Strategy (2023) describes China as a “growing”, “broad and pervasive” threat to the United States (U.S. Department of Defence, 2023).

It is no secret that modern communication technologies and an increasingly digitalized world make it possible to wage war in new, unprecedented ways.

In particular, the Chinese government is currently paying special attention to cyber espionage techniques. Gathering data for foreign intelligence in cyberspace offers a number of advantages that human intelligence cannot objectively offer, including access to large amounts of data that can be easily transferred and also improved protection mode due to the difficulty of identifying the source (Wortzel, 2014).

Espionage, primarily in the form of cyber espionage, can support China's domestic operations and contribute to the development of the national economy, but it can also enable the People's Liberation Army (PLA) to better prepare for any potential military conflict.

The same can be said for China's collection of foreign social data – thus, better understanding the enemy's values, activities, and lines of "polarization" in society can make the task of the military easier.

Recently, the United States has received information that China is accumulating huge amounts of data from various sources for potential future use in numerous ways. This approach is referred to as a "grain of sand" or "mosaic" strategy, which comes from a popular quote in the world of security and covert operations: "If the Russians want to get special sand from a special beach, they will use a submarine. At night, they will swim up, collect a bucket full of sand, take it to the submarine, and leave the beach. The Chinese, on the other hand, will have 500 people picnicking on the beach, each of whom will collect sand in a small jar (or each will take one grain of sand) and bring it back" (Smith, 2023).

Seemingly irrelevant data can be valuable for various social engineering campaigns and future propaganda operations. China is capable of covertly collecting intelligence and conducting espionage operations through corporate proxies and by infiltrating US supply chains.

TikTok can, at least hypothetically, help China collect valuable social data, shape influence over target audiences, track expatriates, and open avenues for future operations under the facade of a harmless platform that fosters creativity. Social media is only one aspect of China's larger efforts to reduce competitive advantage of the United States and establish its own global dominance. China is seeking to penetrate American information ecosystem and physical and technological infrastructure, in particular, through a foreign economic strategy launched in 2013 and widely known as the Belt and Road Initiative.

The Chinese Liberation Army has publicly spoken about the use of social media during the war, which further confirms the ability of TikTok to potentially become a type of new information weapon. So far, the United States has not been able to mitigate the actual and potential threats that TikTok poses to US national security. This thesis leads to the conclusion that TikTok in particular and the broader social media ecosystem in general should be considered as extremely effective tools for intelligence gathering, as well as for conducting targeted information operations and strategic influence on the general public, on the perception of various political, social, and economic processes by society. So, the main thesis is this: the United States must take appropriate measures to protect its citizens, assets, and competitive advantage in the social media ecosystem (Cullen, 2023).

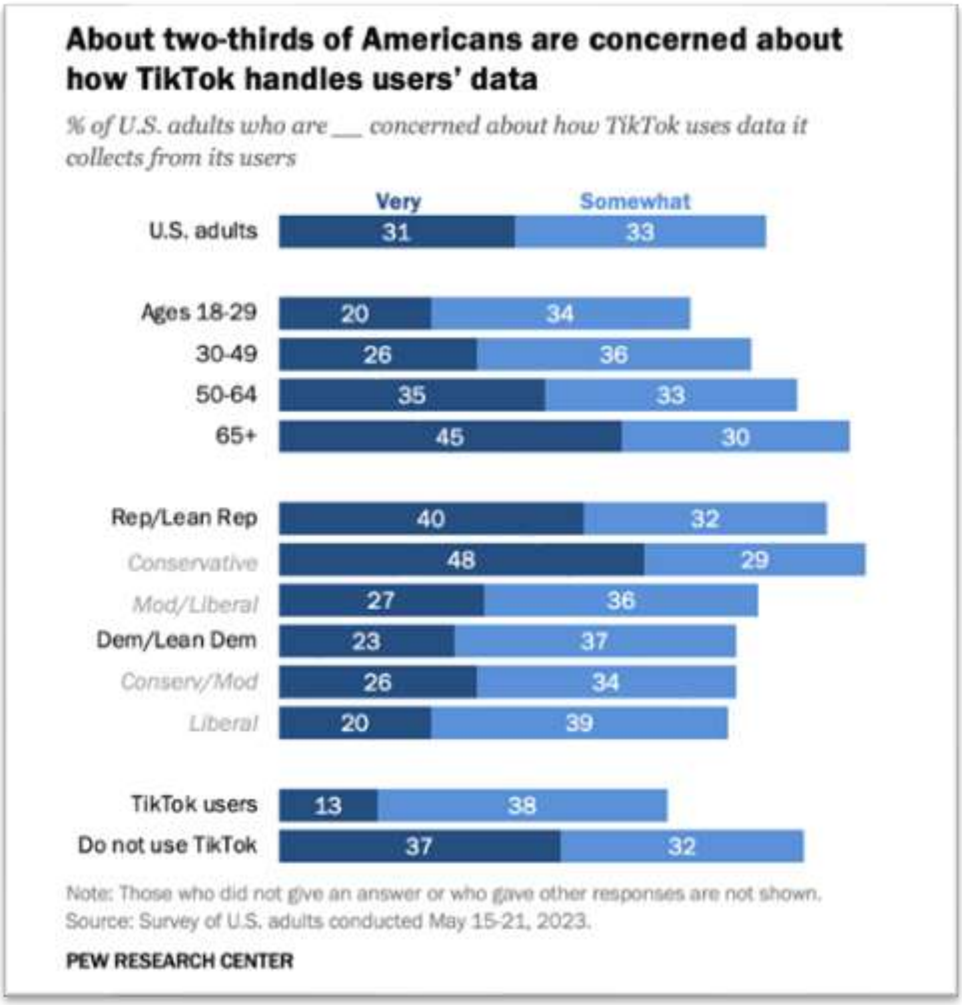

Figure 1. American Survey of citizens on the potential threat of TikTok to national security.
Source: (Pew Research Center, 2023).

Recently, other American researchers have also been paying increasing scholarly attention to the threats that social media pose to national security interests. For example, T. Whelpley writes that, on the one hand, the relatively new and growing phenomenon of social media has many positive consequences for the US national security. It can be used as a means of warning or prevention in military campaigns, such as the war on terror, and as an institutional communication tool. On the other hand, social media can also hinder national security. It plays a controversial role in information warfare, and can be used as a recruitment tool for terrorists, other criminals, and hacktivists willing to spread disinformation and uncontrolled threats. Options for addressing these challenges are as diverse as they are controversial. They range from regulating Internet to exempting social media from any government control. The author summarizes that social media have a more negative impact on national security than a positive one. His recommendations include a more progressive, lawful behavior-oriented self-regulation of the Internet, rather than increased state control (Whelpley, 2014).

In a comparative context, from the standpoint of combining transparency and protecting national interests, it is worth referring to the Draft Law presented on March 25, 2024 in the Ukrainian parliament, which aimed to ban Telegram in Ukraine if the parent company did not introduce certain changes to protect against threats to national security (Verkhovna Rada of Ukraine, 2024).

According to some experts, using Telegram messaging app to send personal data and for official purposes, especially in the public sector and in military zones, is not recommended. Anonymity on the platform is often used to spread false information, he added, including by Russian special services, which negatively affects public order and security in Ukraine (Katsimon & Honcharuk, 2024). This is not to mention the use of Telegram by Russian special services to engage Ukrainian citizens in various forms of cooperation, including reporting locations of the Armed Forces units and military and logistics facilities.

Today, the social network Telegram is actively used, among other things, to cover the war in the Gaza Strip. For example, on October 7, 2023, at 7:14 a.m. local time, the Hamas group al-Qassam Brigades announced on its Telegram channel the launch of a coordinated terrorist attack against Israel. Subsequently, many more vivid posts appeared on both Hamas's Telegram channels and the channels of other Hamas paramilitary groups, which went viral. In just a few hours, the channel's reach has grown by more than 50 percent to 337,000 subscribers (Brooking et al., 2023).

Other global social networks, such as Facebook, X, and TikTok, were also actively used by terrorists to cover their actions. And in the vast majority of cases, such coverage was "distorted" and untrue, aimed at creating false narratives for users. Thus, unlike other social platforms that have introduced very effective mechanisms for restricting certain types of content, Telegram users' channels regularly use the platform to spread and amplify propaganda. Channel owners can choose to unidirectionally broadcast their messages to a wider audience, thus allowing them to tightly control which messages are disseminated through their channels. These controls make Telegram an attractive "first stop" choice for individuals who create and distribute content that can quickly spread to other platforms and reach a wide audience. Already in the first weeks of the propaganda war between Israel and Hamas, this meant that many of the most viral images and videos appeared on Telegram.

In the context of our study, it is also worth noting that the US National Security Strategy, dated October 12, 2022, emphasizes, on the one hand, active and comprehensive support for Ukraine in terms of protection against a full-scale invasion of Russia and further development on democratic and market principles, and on the other hand, the need to strengthen protection against cyber threats of various kinds. It is important to realize that this also applies to potential threats to civil society posed by social networks. The document emphasizes that, as an open society, the United States has a strong interest in strengthening assets that mitigate cyber threats and increase stability in cyberspace. The United States is committed to deterring cyberattacks by state and non-state actors and will continue to respond decisively with all appropriate instruments of national power to hostile actions in cyberspace, including those that disrupt or degrade vital national functions or critical infrastructure. The American position is that this country will continue to promote compliance with the UN General Assembly-endorsed framework for responsible state behavior in cyberspace, which recognizes the key principle: international law applies both online and offline (The White House, 2022).

Conclusions

This research paper underscores the dual nature of social media, which serves as both a platform for free expression and a tool for activities that can jeopardize national security. Through a comparative analysis of global case studies, including the Arab Spring, the 2016 U.S. elections, and protests in Hong Kong, it is evident that social media has become instrumental in shaping political discourse, organizing mass protests, and influencing public opinion. However, these platforms are also frequently exploited for more dangerous purposes, such as spreading disinformation, radicalizing individuals, and coordinating cyberattacks on state institutions.

The role of social media in fostering separatism presents a particular threat to territorial integrity, as seen in various regions where online platforms are used to promote ideologies that challenge state sovereignty and constitutional order. Such a dynamic illustrates the growing complexity of managing security threats in a digital world where geographical boundaries are less relevant.

To mitigate the risks discussed in this paper, there is a pressing need for a balanced approach to the regulation of social media. This must involve not only legal frameworks that address the misuse of these platforms but also enhanced cybersecurity measures to protect critical infrastructure. Moreover, international cooperation is essential to address cross-border disinformation campaigns and other cyber threats that transcend national jurisdictions. While protecting national security, it remains vital to maintain the fundamental freedoms that social media platforms provide, ensuring that measures taken do not stifle legitimate democratic expression.

In conclusion, this research paper highlights a contribution to the ongoing discourse on national security and social media by offering a nuanced perspective on the dual role of social media as both a catalyst for democratic engagement and a potential vector for security threats. This study adds value to the ongoing academic research by integrating comparative global case studies, highlighting emerging security threats,advancing policy recommendations and also referring to the national security debate.

The study underscores the urgent need for robust, adaptable strategies that mitigate the misuse of social media while upholding its role as a space for democratic expression. In our view, such dual emphasis makes the research particularly relevant for contemporary discussions on security policy in the context of rapidly evolving digital technologies and the changing global security landscape.

Bibliographic References

Brooking, E., Mashkoor, L., & Malaret, J. (2023). *Distortion by design: How social media platforms shaped the first stage of the Mideast crisis*. Atlantic Council. https://view.atlanticcouncil.org/social-media-gaza/p/1#6583344f5597b

Chernysh, R., Chekhovska, M., Stoliarenko, O., Lisovska, O., & Lyseiuk, A. (2023). Ensuring information security of critical infrastructure objects as a component to guarantee Ukraine's national security. *Amazonia Investiga, 12*(67), 87–95. https://doi.org/10.34069/AI/2023.67.07.8

Chukwuere, J., & Onyebukwa, C. (2018). The Impacts of Social Media on National Security: A View from the Northern and South-Eastern Region of Nigeria. *International Review of Management and Marketing, 8*(5), 50-59. Retrieved from: https://www.econjournals.com/index.php/irmm/article/view/6852/pdf

Cox, J., & Koebler, J. (2019). *Facebook Bans White Nationalism and White Separatism*. Vice. Retrieved from: https://www.vice.com/en/article/nexpbx/facebook-bans-white-nationalism-and-white-separatism

Criminal Code of Ukraine. *Criminal Code of the Republic of Ukraine*, September 1, 2001. Retrieved from: https://acortar.link/kviors

Cullen, B. (2023). *Assessing the Threat of Social Media to National Security: Information Operations in the 21st Century*. Senior Theses. Retrieved from: https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=1665&context=senior_theses

Eriksen, T. H. (2007). Nationalism and the Internet. *Nations and nationalism, 13*(1), 1-17. URL: https://onlinelibrary.wiley.com/doi/full/10.1111/j.1469-8129.2007.00273.x

Ganesh, B., & Bright, J. (2020). Countering Extremists on Social Media: Challenges for Strategic Communication and Content Moderation. *Policy and Internet, 12*(1), 6-19. https://doi.org/10.1002/poi3.236

Horska, K., Dosenko, A., Iuksel, G., Yuldasheva, L., & Solomatova, V. (2023). Internet platforms as alternative sources of information during the Russian-Ukrainian war. *Amazonia Investiga, 12*(62), 353–360. https://doi.org/10.34069/AI/2023.62.02.36

Hussain, N. (2008). *The Role of Media in National Security: A Case Study of 1998 Nuclear Explosions by Pakistan*. SASSI Research Report 20. https://www.files.ethz.ch/isn/128264/Report-20.pdf

Iqbal, A. R. (2011). *Social Mobilisation and Online Separatist Movement in Balochistan*. Margalla Papers, 126-150.

Kamensky, D., Dudorov, O., Savchenko, A., Movchan, R., & Danylevska, Y. (2023). Criminal liability for humanitarian aid embezzlement during war: The case of Ukraine: Responsabilidad penal por malversación de ayuda humanitaria durante la guerra: el caso de Ucrania. *Cuestiones Políticas, 41*(77), 760-776. https://doi.org/10.46398/cuestpol.4177.50

Kasi, A., Kasi, M., & Qadir, A. (2021). The Effects of Social Media on National Security: An Overview. *Global Strategic & Security Studies Review, VI*(I), 121-127. https://doi.org/10.31703/gsssr.2021(VI-I).13

Katsimon, O., & Honcharuk, L. (2024). *"Telegram has killed the remnants of its reputation" – Center for Strategic Communications on the blocking of Ukrainian chatbots*. Suspilne.media. https://acortar.link/OWMkv5

Lutsenko, Y., Motyl, V., Tarasiuk, A., Areshonkov, V., Diakin, Y., & Kamensky, D. (2023). Globalization of White-Collar Crime: Far and Beyond National Jurisdictions: Globalización de la delincuencia de cuello blanco: Más allá de las jurisdicciones nacionales. *Political Questions, 41*(76), 64-75. https://doi.org/10.46398/cuestpol.4176.03

Marcellino, W., Johnson, C., Posard, M., & Helmus, T. (2020). *Foreign Interference in the 2020 Election: Tools for Detecting Online Election Interference.* Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RRA704-2.html

Myroshnychenko, V., Kamensky, D., Lysenko, T., Makarenko, T., & Petiahina, I. (2024). "Defense of Ukraine" degree program for future school teachers: a new element of Ukrainian higher education. *Revista Eduweb*, *18*(1), 190-203. https://doi.org/10.46502/issn.1856-7576/2024.18.01.14

Movchan, R., Vozniuk, A., Kamensky, D., Koval, I., & Golovko, O. (2022). Criminal and legal protection of land resources in Ukraine and Latin America: comparative legal analysis. *Amazonia Investiga*, *11*(51), 328-336. https://doi.org/10.34069/AI/2022.51.03.33

Pew Research Center (2023). *Majority of Americans say TikTok is a national security threat, but this varies by party, ideology and age*. https://acortar.link/6bNS4b

Siddique, A. (2024). *What's Behind the Deadly Surge of Violence in Pakistan's Balochistan?* Radio Free Europe. https://www.rferl.org/a/pakistan-balochistan-separatists-baluch/32917725.html

Smith, H. (2023). *Chinese spies are targeting access, not race*. Foreign Policy. https://foreignpolicy.com/2023/09/22/china-spying-race-intelligence-targeting

The White House (2022). *National Security Strategy*. https://acortar.link/EQClpW

U.S. Department of Defence (2023). *The 2023 Department of Defense Cyber Strategy Summary (2023)*. https://acortar.link/8zwfPW

Vasu, N., Ang, B., Jayakumar, S., Faizal, M., & Ahuja, J. (2018). *Fake News: National Security in the Post-Truth Era. Policy Report.* https://www.rsis.edu.sg/wp-content/uploads/2018/01/PR180313_Fake-News_WEB.pdf

Verkhovna Rada of Ukraine (2024). *Draft Law on Amendments to Certain Laws of Ukraine on Regulation of Activities of Information Sharing Platforms Through which Mass Information is Disseminated.* https://itd.rada.gov.ua/billInfo/Bills/Card/43884

Whelpley, T. (2014). *The Effects of Social Media on U.S. National Security*. MSU Graduate Theses. https://bearworks.missouristate.edu/theses/1492

Wortzel, L. M. (2014). *The Chinese People's Liberation Army and Information Warfare*. Strategic Studies Institute, US Army War College. http://www.jstor.org/stable/resrep11757