Revealing Hybrid Threats: Vulnerability Exploitation in Romania's Social Media Landscape

Georgiana-Daniela Lupulescu
National Defense University "Carol I", Bucharest, Romania

geo.lupulescu@yahoo.co.uk

Abstract: Taking a deep look into hybrid operations characteristics, an important and omnipresent one is targeting vulnerabilities mode of action. As the global landscape evolves and challenges national security like never before, understanding the mechanisms state and non-state entities use to exploit vulnerabilities becomes paramount. By examining the contemporary geopolitical contexts, this article sheds light on the multifaceted strategies deployed by various actors through social media platforms to undermine the resilience of the Romanian state. Due to its geographical location, Romania is not only a major pillar for regional security but also has an important strategic role in maintaining security in both NATO and UE. Exploiting Romania's security weaknesses may be the way hybrid actors pursue their geopolitical interests, ideological aims, and regional power struggles. At the beginning of the study, a short framework will be presented for the concept of vulnerabilities within a state, focusing on the security weaknesses that emerge from several domains, such as economic, political, technological, and in particular social susceptibilities, and how they manifest in social media. Following, the article will include methods and tactics used in social media, by various types of actors, considering the use of cyber-attacks, disinformation campaigns, covert influence, or economic coercion for a clearer image of the target-attack binomial. Furthermore, a short analysis of Romania's exposure to hybrid threats will be provided. Starting from the research hypothesis that Romania's geopolitical and geographical location is the key factor in establishing its vulnerability degree to hybrid threats manifestation, the main question that emerges is how to minimize its vulnerabilities. The methodology that will be used in conducting this research includes a short literature review of the concept of vulnerabilities within a state, as well as weaknesses exploitation through social media, followed by the case study analysis where we will be focusing on some of Romania's vulnerabilities within social media. Through this comprehensive examination, this article underscores the significance of recognizing and addressing vulnerabilities within a state, particularly in the context of evolving global challenges and threats to national security. It emphasizes the strategic importance of Romania in maintaining regional and international security. The article serves as a wake-up call to the potential dangers posed by hybrid actors who exploit these vulnerabilities using social media platforms, urging Romania and its allies to take proactive measures to bolster their defense and resilience against these multifaceted threats.

Keywords: Vulnerability, Disinformation, Resilience, Security weaknesses, Social media

1. Introduction

Hybrid operations seem to be omnipresent in the current global environment. Even if we talk about the continuous existence of hybrid threats or the outbreak of a conflict, there are certainly elements of hybrid operations included. The hybrid term does not have a very long history as Frank Hoffman first defined it (2007) at the beginning of the 2000s from the necessity of naming the change in terms of actors involved, instruments used, and of course the combination of all that we previously knew, or, as Treverton et. al. said: "they differ from previous conflict more in degree than in kind" (Treverton, et al., 2018).

Many authors have tried defining hybrid threat, hybrid war, or hybrid operations, each of them coming with a new point of view, not as much different from other authors'. For example, Hoffman (2007), Bilal (2021), or the experts from Both the European Parliament and the Council (2016) focused on the fusion of regular and irregular warfare taking into account the methods, instruments of power, and actors involved. At the same time, some authors focus on the vulnerability-targeting characteristic of hybrid operations, as a way of achieving strategic goals. This is supported also by Cullen and Reichborn-Kjennerud who emphasize the not-so-new character, but also the shift in terms of synchronization of the instruments of power and the "exploitation of creativity, ambiguity, non-linearity, and the cognitive elements of warfare" (Cullen & Reichborn-Kjennerud, 2017).

In the hybrid operations discussion, one important aspect seems to be that it exceeds borders, so there are many casualties beyond the attacked state. This is of utmost importance when preparing for or facing threats. It shows us that we need to be united and work together, but it also means that the battlefield has changed. Nowadays a website or a social media platform may be a promising environment for hybrid actors to initiate actions from the hybrid operations spectrum.

This article sheds light on the strategic importance of the geopolitical role of Romania in maintaining regional security. The geographical position at the eastern border of both NATO and EU, Romania has and will always have a crucial role for the stability and security of the alliances. Besides the measures taken for military defense

such as the multinational bases or the anti-missile shield, there is a tremendous need for actions against hybrid threats or even a possible hybrid operation.

Vulnerability is the key element of hybrid operations targets. When assessing the risk to security, posed by hybrid operations, one should not only look at the possible threats or actors with the means and intent to do that but also at the weaknesses in its own political, military, economic, social, informational, and infrastructure (PMESII) domains. The vulnerabilities within a state could determine the capacity to face and counteract hybrid threats, but not all the weak points need to be exploited, that only happens if it helps the greater goal of hybrid actors. Focusing on Romania's vulnerabilities, I will emphasize those from the PMESII domains that could be exploited through social media platforms. Moreover, the hybrid operations tools used against Romania and its allies using social media platforms as a dissemination channel must be named, acknowledged, and counteracted as fast and as efficiently as possible.

My research will outline some of the methods, tactics, and tools used by hybrid actors in the online environment and a few recommendations to reinforce our resilience in various ways, diminishing our vulnerabilities or strengthening our defense.

1.1 Framework of Vulnerabilities

The national security level within a state is defined by its risk-vulnerability-threat triad. The concept of vulnerability in the acceptance of The National Defense Strategy of Romania for the 2020-2024 period is defined as: "functional-systemic/structural deficiencies that can be exploited or can contribute to the materialization of threats or risks, weakening the state's ability to reduce the impact of events with the potential to seriously affect the normal functioning of its institutions, the life and physical integrity of citizens and the organization of human communities, as well as the capacity to protect, defend and promote national security values, interests, and objectives" (Administrația Prezidențială, 2020). The concept of vulnerabilities within a state is a complex and multifaceted domain, encompassing various dimensions that can be exploited by external actors for strategic, ideological, or geopolitical purposes. Understanding these vulnerabilities is essential for devising effective strategies to fortify a nation's resilience against hybrid threats.

One very important characteristic of hybrid actions is that often they target vulnerabilities from different domains at the same time, achieving a synergic effect. Rarely the main goal will be to create social division, for example. Certainly, there will be some hidden objectives such as diminishing the trust in government institutions or manipulating the population's perception and so being more susceptible to believe and act like they are told by various actors. The affirmation is supported by Petrescu, who sees the hybrid threat as a holistic one, and not as a sum of threats (Petrescu, 2019), which means that usually there is a main strategic goal, the resources and instruments are used innovatively and unpredictably, and the PMESII domains may be subject to attack, all at the same time. Understanding the interplay of the vulnerabilities is crucial for assessing a state's overall susceptibility to hybrid threats. It is important to recognize that the vulnerabilities are often interconnected, and exploitation in one domain may have cascading effects across others.

Simultaneously, while a system may exhibit vulnerabilities, it doesn't automatically render itself susceptible to targeting. The critical factor lies in the existence of a strategic objective that a hybrid actor seeks to attain. Moreover, the pivotal element is the discernible intent to orchestrate a hybrid operation. In essence, the mere presence of vulnerabilities does not precipitate targeting; it is the alignment with a larger strategic purpose and a deliberate intent that sets the stage for potential hybrid engagement.

In this research paper, it is imperative to underscore that our focus diverges from the prevalent discourse on vulnerabilities within networks, informational systems, and computers—subjects extensively covered in the existing literature. We intentionally navigate away from the well-trodden path of cyber-related vulnerabilities, recognizing that the mere existence of such weaknesses does not inherently imply susceptibility to hybrid operations. Instead, our emphasis lies on discerning and elucidating the strategic motives and intentions that drive hybrid actors, acknowledging that vulnerability exploitation in the digital realm does not automatically translate into, or exclusively predicate, the orchestration of a hybrid operation. By delving into this nuanced perspective, we contribute a distinct angle to the broader discourse on security and hybrid threats, enriching the understanding of the multifaceted dynamics involved.

Some of these vulnerabilities within a state, that could be exploited by hybrid actors for each of the PMESII domains are presented in the figure below, with the specification that usually these are mixed and interconnected and the hybrid actors exploit more than one vulnerability at a time.

Figure 1: Vulnerabilities in the PMESII domains

As we may see in the figure above, any disorder, any weakness or any other factor that negatively impact the well being of a system or its proper functioning, may constitute into a vulnerability exploitable by hybrid actors. Let's take for example the training gaps in the military domain. Besides its evident harmful impact in terms of inappropriate use of equipment, high injury or mortality rates, and minimum chances of winning a battle, training gaps may be exploited by hybrid actors in various ways. Such an example could be the annexation of Crimea in 2014. The Ukrainian military had undergone significant restructuring and downsizing following the dissolution of the Soviet Union. This restructuring resulted in gaps in training, equipment, and readiness, particularly in areas such as cyber defense, intelligence gathering, and unconventional warfare.

Russian hybrid actors exploited these gaps by launching a sophisticated cyber warfare campaign against Ukrainian military and government infrastructure, disrupting communications, intelligence gathering, and command and control systems. Additionally, Russian propaganda efforts spread disinformation to sow confusion and undermine morale among Ukrainian military personnel.

Furthermore, the Ukrainian military's training and preparedness for unconventional warfare and irregular tactics were not adequately developed, leaving them ill-prepared to counter the hybrid tactics employed by Russian-backed forces, including irregular troops and local separatist militias. Or, as Renz (2016) said: „Ukraine did not have corresponding capabilities and did not even attempt to put up a military resistance". Since then, they adopted reforms across various levels, encompassing tactical and strategic measures, which incorporate both political initiatives such as enhancing transparency, combating corruption, and ensuring civilian oversight of the military, as well as military-focused reforms like modernizing equipment, restructuring command and control, and enhancing professionalism (Bowen, 2022).

The manifestation of vulnerabilities in social media represents a complex and dynamic challenge in today's interconnected digital landscape. Social media platforms, while serving as powerful tools for communication and information sharing, also become breeding grounds for various vulnerabilities that can have wide-ranging consequences. The big change with everyone using social media a lot is how quickly things get shared in real

time, and nearly everyone can do it. It means news and updates can spread instantly, breaking down borders and letting people from anywhere connect. People create and share a ton of content, letting anyone have a say in global discussions. Social media makes information go viral fast, shaping public talk and sparking movements in no time. But it also brings challenges like figuring out if what you see is true. With constant access to social media, individuals can express themselves, share their stories, and support different causes. This makes everyone's voice matter, challenging the usual power structures. However, there's also the downside of non-stop connection, leading to an overload of information. Steingartner et. al. also stipulate that "although lies and manipulations in public information space are not a novelty, the quantity and speed of spreading misinformation, especially through social networks and mobile communication applications present an unprecedented challenge." (Steingartner, et al., 2022) Thus, while social media's real-time sharing and broad access bring new opportunities, they also bring new issues that we need to navigate in this digital age.

Unlike other types of vulnerabilities, such as the ones presented above, in social media platforms, people are the weak link and most of the tools used aim to manipulate and influence people's perceptions, thoughts, and opinions (Bruning, et al., 2020). Both state and non-state actors use social media platforms for spreading false and misleading information and the enormous success of their operations is due to very efficient algorithms that take into account all individuals' characteristics such as sex, race, age, ethnicity, culture, religion, preferences, etc. sharing specific messages that impact a certain target.

Vulnerabilities within social media must be viewed from two distinct perspectives, one regarding the system security vulnerabilities, and the other from a social perspective. Even though the first has great influence on the second we will refer only to the social vulnerabilities emerging through social media. For example, CSO's online website provides 15 cases of data breaches from the past few years involving the exposure or selling of users' personal information (Hill & Swinhoe, 2022). As we may see, even great companies, like Yahoo, Facebook, or LinkedIn could be and were vulnerable. Every vulnerability could eventually become the point of entry for those with malicious intent, such as hybrid actors.

The vulnerabilities presented in the figure below could also be considered as threats as they require a malicious actor to initiate and exploit the weaknesses caused especially by the lack of security education and culture, but also by the absence of robust cybersecurity measures. These vulnerabilities not only expose potential points of entry for malicious actors but also highlight the critical role that the human factor plays in exacerbating the overall threat landscape. Additionally, the inadequacy of cybersecurity measures further amplifies the risk, creating an environment where vulnerabilities can be easily exploited. It underscores the importance of comprehensive security strategies that encompass both technological safeguards and an emphasis on fostering a security-conscious culture among users and stakeholders.

Furthermore, Al Hasib (2009) also views the weaknesses exploitable through social media as threats, which he divides into:

- Privacy-related threats which include digital dossier of personal information, face recognition, content-based image retrieval, image tagging and cross-profiling, and difficulty of complete account deletion;
- SNS Variants of Traditional Network and Information Security Threats which include: spamming, cross-site scripting, viruses and worms, and SNS (social networking service) aggregators;
- Identity-related threats: phishing, information leakage, and profile squatting through identity theft;
- Social threats: stalking or corporate espionage.

At the same time, according to Amanda Hetler (2023) six of the most common social media privacy issues are:

- Data mining for identity theft;
- Privacy setting loopholes;
- Location settings;
- Harassment and cyberbullying;
- False information;
- Malware and viruses.

We provide another list of possible threats/exploitable vulnerabilities through social media. These are just a few examples of instruments that hostile actors could use to obtain something, either money or some other material goods, or another kind of strategic advantage like influencing elections (Berghel, 2018).

Figure 2: Vulnerabilities within social media platforms

Addressing these manifestations of vulnerabilities in social media requires a multi-faceted approach involving technological advancements, robust security measures, user education, and policy frameworks. As social media continues to play a pivotal role in modern communication, understanding and mitigating these vulnerabilities are crucial for fostering a safer and more secure digital environment.

2. Social Media as a Battlefield

In the digital age, social media has evolved into a complex battlefield where ideas, narratives, and influences clash on a global scale. There are plenty of examples, one being the influence of social media in the elections (Davis & Taras, 2022). Far from being mere platforms for social interaction, these networks have become strategic arenas for individuals, groups, and nations to shape public opinion, influence political landscapes, and

advance their agendas. Hybrid actors make no exception as the use of propaganda and disinformation has increased on social media platforms. Besides the evident advantage of low cost-high impact, the use of social media platforms provides the hybrid actors the anonymity, ambiguity, and deniability they desire.

Hybrid actors, state, non-state, or a combination of those, including proxy, auxiliary, surrogate, and affiliated forces (Rauta, 2019) employ all the instruments, both conventional and unconventional blending forces, means, purposes, and targets in pursuing a strategic goal. They often present the following characteristics:

- Combination of resources, capabilities, and strategies of both state and non-state entities, leveraging the strengths of both sectors;
- They operate across multiple domains, including military, economic, political, informational, and cyber. They seamlessly integrate these domains to achieve their objectives, making it challenging for traditional military and defense structures to respond effectively;
- They involve asymmetric tactics, where unconventional methods are used to exploit the weaknesses of more conventionally organized opponents. This can include guerrilla warfare, insurgency, and cyber-attacks;
- Hybrid actors often operate in a gray zone, deliberately maintaining ambiguity about their involvement in certain activities. This allows them to deny responsibility, making it difficult for adversaries to respond decisively;
- They manipulate information to shape perceptions, influence public opinion, and create confusion. This includes the use of propaganda, disinformation, and cyber operations to control the narrative;
- They can quickly adjust their tactics and strategies in response to changing circumstances, taking advantage of emerging opportunities or adapting to countermeasures employed by adversaries.

Hybrid actors represent a dynamic and evolving challenge in the contemporary geopolitical landscape. Understanding their characteristics and tactics is essential for developing comprehensive strategies to address the complex nature of hybrid warfare. According to Giannopoulos et. al. “the activity behind Hybrid Threats is undertaken particularly by actors with more or less authoritarian or totalitarian views of power” (Giannopoulos, et al., 2021), and this relates to what we emphasized before, the fact that on one hand, they utilize specific instruments and tools, difficult to anticipate or to counteract by the attacked state and, on the other hand, they manage to disguise their goals and even their identities.

There are plenty of examples of hybrid actors who engaged in hybrid operations within social media but we will remember just a few of them.

First of all, we have to take a look at the Russian Interference in the U.S. elections, particularly during the 2016 presidential campaign, which has been the subject of extensive investigation and scrutiny. The interference involved a combination of social media manipulation, hacking, and the dissemination of disinformation. Furthermore, the Annual Threat Assessment of the US Intelligence Community shows that Russia continued with the influence operations against elections, the most recent one being in the 2022 U.S. midterm elections (2023).

The second state actor to consider is China, which has been accused of conducting influence operations on social media platforms to shape global narratives in its favor. This includes the use of state-controlled media outlets, paid trolls, and coordinated campaigns to spread positive information about China and counter-narratives perceived as unfavorable to the Chinese government. Lots of studies have been conducted regarding Chinese influence but according to Diamond and Schell, “China has not sought to interfere in a national election in the United States or to sow confusion or inflame polarization in our democratic discourse the way Russia has done” (Diamond & Schell, 2019);

Third, Iranian disinformation campaigns must be taken into account as they are aimed at advancing Iranian geopolitical interests, including the creation of fake accounts and the dissemination of misleading content to influence public opinion on issues such as regional conflicts, international relations, and a more evident one, COVID-19. Iran has conducted a massive disinformation campaign about COVID-19, telling lies about the gravity and consequences and bringing as proof false health reports and accusations against other countries (Dubowitz & Ghasseminejad, 2020).

And last, extremist groups, which are considered to be non-state hybrid actors, such as ISIS, have used social media for recruitment and propaganda purposes. These hybrid operations involve disseminating extremist ideologies, recruiting sympathizers, and coordinating activities. Platforms like Twitter and YouTube have faced challenges in combating the spread of such content. A study that analysed 100 Facebook pages and 50 Twitter

user accounts has shown that groups like ISIS use social media for recruitment and propaganda, using violent videos and hate speech (Awan, 2017).

Social media, once envisioned as a tool for connecting people and sharing ideas, has transformed into a multifaceted battlefield where information warfare is waged. Understanding the methods and tactics employed in this digital arena is crucial for users to navigate the landscape critically and for policymakers to develop effective strategies to mitigate the negative impacts on society. As social media continues to evolve, the challenge lies in finding a balance between preserving freedom of expression and protecting the public from manipulation and disinformation.

3. Romania's Strategic Vulnerabilities

Romania's geographical location at the crossroads of Europe, along with its membership in NATO and the EU, positions it as a key player in regional security, trade, and cooperation. The country's historical and contemporary importance reflects its multifaceted role in shaping the dynamics of Eastern and Southeastern Europe. Romania is situated at the northern entrance to the Balkan Peninsula, serving as a gateway between Central Europe and the Balkans. Its geographical position has historically made it a bridge between different cultural, economic, and political influences in the region. Moreover, the Carpathian Mountain and the Black Sea access increase its strategic importance for both NATO and the EU's defense against any Eastern interference.

Although both NATO and EU recognize and value Romania's strategic geopolitical locations, some authors believe that Romania does not take full advantage of it and that its great location and a great variety of natural resources are not fully reflected in the country's economy and people's wellbeing (Banea, 2016). Furthermore, Moga and Bureiko argue that even though Romania aspires to a greater status (Administrația Prezidențială, 2020), "the country has so far only displayed a 'small power' behavior" (Moga & Bureiko, 2022).

Furthermore, Banea emphasizes the fact that it is the population's consciousness and education that influence and even determine the position on the global scale (Banea, 2016). This perspective delves into how the collective mindset and educational levels of a society can significantly impact its ability to navigate the complexities of the international arena. There is a huge difference between a well-informed population about global issues, which possesses a nuanced understanding of cultural differences, and demonstrates a high level of social consciousness, and a population that is not interested in geopolitics, security, or the global market. While high levels of consciousness and education empower the state to actively engage in global affairs and contribute positively, a country where the population is not actively involved, faces challenges that may impact its diplomatic, economic, and cultural standing on the international stage. This underscores the critical importance of investing in education and fostering a collective consciousness that enables nations to navigate and thrive in an interconnected world.

At the same time, we must take a look at Romania from the other point of view, the one where its current status was given by its membership in the NATO and EU. Some authors seem to believe that its strategic importance has increased due to the new roles given by the alliances (Moga & Bureiko, 2022).

So, the question remains. Is Romania important in the international security arena due to its geographical position and its internal capabilities or due to its membership in NATO and the EU? We believe that Romania's importance in the international security arena is a result of the intricate interplay between its geographical position, internal capabilities, and memberships in NATO and the EU. A comprehensive understanding of these dynamics is crucial for addressing vulnerabilities and ensuring the nation's continued role as a key player in regional and global security efforts. Continuous efforts to strengthen both internal capacities and international collaborations will contribute to Romania's resilience and effectiveness in the evolving landscape of international security.

We have identified four major pillars which can be viewed on one hand as potential vulnerabilities, and on the other hand as key solutions for strengthening Romania's national security and increasing its role, especially in the regional security framework.

Figure 3: Security pillars

Given the interconnected nature of the modern world, Romania faces cybersecurity challenges that require ongoing attention. Strengthening capabilities to protect against cyber threats is essential for safeguarding national security. While there are lots of threats that could manifest in social media, such as disinformation campaigns, phishing and social engineering, spread of malicious software, identity theft, or manipulation of public perception, besides cyber-attacks, enhancing cybersecurity measures plays a fundamental role. Moreover, robust cybersecurity measures are essential for safeguarding critical infrastructure, including energy grids, transportation systems, and communication networks. Cybersecurity has become an important topic for researchers worldwide as there is plenty of scientific research on networks, security vulnerabilities, threat detection and mitigation strategies, encryption technologies, risk assessment methodologies, incident response protocols, and the development of advanced cybersecurity tools and frameworks. Researchers are actively exploring innovative approaches to address the evolving landscape of cyber threats, ranging from sophisticated cyberattacks to emerging challenges in areas such as the Internet of Things (IoT), artificial intelligence (AI), and cloud computing security. This wealth of research is crucial for enhancing the resilience of digital ecosystems, protecting sensitive data, and fortifying the global cybersecurity infrastructure against constantly evolving cyber risks (Schiappa, et al., 2019), (Sabottke, et al., 2015), (Ozkaya, 2018), (Walter, 2023).

Romania has initiated measures to strengthen its cybersecurity posture, Hackout.ro is just one small example. They started a series of Hackout Talks, as they call them, where specialists from the cyber security field give presentations to raise public awareness of the risks and threats in the online space. Moreover, the Hackout team publishes a series of articles, with the same goal, education and public awareness (Harvat, et al., 2023).

The second pillar, which is both a potential vulnerability and a source of enhancing Romania's security is the energy field and the fact that Romania, despite its energy resources, is still dependent on external energy sources. Diversifying energy sources and ensuring resilience against disruptions may bring huge contributions to national security. A study about the security incidents caused by interruption of electricity supply was conducted by the, besides other specific conclusions, they stipulate that there is a tendency to integrate the communication field among essential services for the functioning of societies as a whole (National Authority for Administration and Regulation in Communications, 2021).

Another important pillar is represented by the regional relations. Romania's President, Klaus Iohannis argues that: "the development of Strategic Partnerships and other bilateral relations, the promotion of the strategic relevance of the Black Sea, the projection of Romania's profile as a factor of stability and the promotion of EU values in the region, as well as the support of political, economic and security interests in areas of interest for our country will be concrete benchmarks of Romania's foreign policy actions" (Iohannis, 2023). Thus, actively managing and fostering positive relations with neighbouring countries can mitigate potential vulnerabilities and contribute to regional stability.

The last pillar, social cohesion and resilience, especially in Romania's case, may have needed to be analysed in a much larger paper as it seems to be the universal answer to all our challenges posed especially by hybrid threats. Romania faces social media challenges that impact its social cohesion and resilience. Despite these challenges, Romania's historical resilience and shared cultural identity contribute to its ability to counteract divisive influences. Fostering digital literacy, promoting media literacy, and enhancing cybersecurity measures are crucial steps for Romania to strengthen social cohesion in the digital age and build resilience against the negative impacts of social media challenges. Moreover, The Social Alternatives Association has conducted a study named *Fake News – Fake Reality: Social Resilience through Critical Thinking* with the main purpose of establishing the first anti-fake news coalition in Central and Eastern Europe (The Social Alternatives Association, 2023).

A similar study on state vulnerabilities within social media was conducted by Faruk Hadžić (2020) in Bosnia and Hertzegovina. Among his conclusions was the imperious need of a broader national security strategy with a great focus on cybersecurity and the increase of vulnerabilities in the cyber domain. Moreover, the appearance of new types of crimes due to social media development entails competent law enforcement institutions, well-trained and equipped, and which act under precise and thorough regulations.

4. Conclusions

The research emphasizes the interconnected and multifaceted nature of vulnerabilities within a state, acknowledging that hybrid actors exploit diverse domains simultaneously. The holistic approach aligns with the idea that hybrid threats often have a main strategic goal, employing innovative and unpredictable methods across various domains. Recognizing the interconnectedness of vulnerabilities is crucial for assessing a state's susceptibility to hybrid threats. The presence of vulnerabilities alone does not precipitate targeting; it is the alignment with a larger strategic purpose and deliberate intent that sets the stage for potential hybrid engagement.

In the context of social media, vulnerabilities take on a unique dimension, often exploiting the human factor. The vulnerabilities identified, including misinformation and manipulation, underscore the challenges posed by the rapid spread of information in real-time. Social media platforms become arenas for influencing perceptions, leveraging efficient algorithms to target specific demographics. Addressing these vulnerabilities requires technological advancements and a comprehensive approach involving user education, policy frameworks, and robust cybersecurity measures. The interplay of human factors, technological safeguards, and security-conscious culture is essential in mitigating the risks associated with social media vulnerabilities.

Romania's global importance results from its strategic location, internal capabilities, and NATO-EU memberships. Balancing geopolitical advantages and alliances is crucial for sustained regional and global influence and strengthening internal capacities and international collaborations is pivotal for resilience. For that, Romania could focus its efforts on four key pillars for national security: robust cybersecurity, diversified energy sources, positive regional relations, and social cohesion and resilience. Initiatives like Hackout.ro showcase proactive steps in cybersecurity, while strategic efforts in energy and regional partnerships contribute to overall security.

References

Administrația Prezidențială, 2020. Strategia Națională de Apărare a țării pentru perioada 2020-2024, București: s.n.

Al Hasib, A., 2009. Threats of Online Social Networks. IJCSNS International Journal of Computer Science and Network Security, 9(11), pp. 288-293.

Awan, I., 2017. Cyber-extremism: Isis and the power of social media. Society, 54(2), pp. 138-149.

Banea, C. B., 2016. Romania: Geographical and Geopolitical Position. Annals of the University of Oradea, Economic Science Series, 25(2).

Berghel, H., 2018. Malice domestic: The Cambridge analytica dystopia. Computer, 51(05), pp. 84-89.

Bilal, A., 2021. Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. NATO Review, 30 November.

Bowen, A. S., 2022. Ukrainian Armed Forces, s.l.: Congressional Research Service.

Bruning, P. F., Alge, B. J. & Lin, H.-C., 2020. Social networks and social media: Understanding and managing influence vulnerability in a connected society. Business Horizons, Volume 63, pp. 749-761.

Cullen, P. J. & Reichborn-Kjennerud, E., 2017. MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare, s.l.: s.n.

Davis, R. & Taras, D., 2022. Electoral Campaigns, Media, and the New World of Digital Politics. In: s.l.:Ann Arbor> University of Michigan Press, pp. 1-22.

Diamond, L. & Schell, O. eds., 2019. China's influence and American interests: Promoting constructive vigilance. s.l.:Hoover Press.

Dubowitz, M. & Ghasseminejad, S., 2020. Iran's COVID-19 disinformation campaign. CTC Sentinel. United States Military Academy.

European Commission, 2016. Joint Framework on countering hybrid threats - a European Union response, Brussels: s.n.

Giannopoulos, G., Smith, H. & Theocharidou, M., 2021. The lanscape of hybrid threats: A conceptual model. Luxembourg: Publications Office of the European Union.

Hadžić, F., 2020. The Influence of Social Media on Threats to Identity, Stability and National Security; Institutional Inefficiency and Vulnerability of B&H. Defendology, Issue 45-46, pp. 67-109.

Harvat, A., Puiu, G., Pitiș, D. & Galea, V., 2023. HACKOUT. Cyber Attacks Portal. [Online] Available at: https://hackout.ro [Accessed 28 December 2023].

Hetler, A., 2023. 6 common social media privacy issues. [Online] Available at: https://www.techtarget.com/whatis/feature/6-common-social-media-privacy-issues [Accessed 28 02 2024].

Hill, M. & Swinhoe, D., 2022. The 15 biggest data breaches of the 21st century. [Online] Available at: https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html [Accessed 28 02 2024].

Hoffman, F., 2007. Conflict in the 21st century: The Rise of Hybrid Wars. Arlington(Virginia): Potomac Institute for Policy Studies.

Iohannis, K., 2023. Commitments. Foreign policy. [Online] Available at: https://www.presidency.ro/en/commitments/foreign-policy[Accessed 28 December 2023].

Moga, T. L. & Bureiko, N., 2022. Ambitions yet unrealized: Romania's status and perceptions from the immediate eastern neighbourhood. Southeast European and Black Sea Studies.

National Authority for Administration and Regulation in Communications, 2021. Study on incidents of security caused by interruption of supply electricity, s.l.: s.n.

Office of the Director of National Intelligence, 2023. Annual Threat Assessment of the US Intelligence Community, s.l.: s.n.

Ozkaya, E., 2018. Cybersecurity Challenges in Social Media, s.l.: s.n.

Petrescu, D.-L., 2019. The Hybrid Threat - Action and Counteraction. Bucharest, "Carol I" National Defence University.

Rauta, V., 2019. Towards a typology of non-state actors in „Hybrid Warfare": Proxy, auxiliary, surrogate and affiliated forces. Cambridge Review of International Affairs.

Renz, B., 2016. Russia and 'hybrid warfare'. Contemporary Politics.

Sabottke, C., Suciu, O. & Dumitraș, T., 2015. Vulnerability Disclosure in the Age of Social Media: Exploiting Twitter for Predicting Real-World Exploits. Washington, D.C., s.n.

Schiappa, M., Chantry, G. & Garibay, I., 2019. Cyber Security in a Complex Community: A Social Media Analysis on Common Vulnerabilities and Exposures. s.l., s.n.

Steingartner, W., Možnik, D. & Galinec, D., 2022. Disinformation Campaigns and Resilience in Hybrid Threats Conceptual Model. Poprad, 2022 IEEE 16th International Scientific Conference on Informatics (Informatics), pp. 287-292.

The Social Alternatives Association, 2023. Social Alternatives. [Online] Available at: https://www.alternativesociale.ro/fake-news-fake-reality-2/[Accessed 19 December 2023].

Treverton, G. F. et al., 2018. Addressing Hybrid Threats. s.l.:Swedish Defence University.

Walter, A. T., 2023. Cyber Security and Social Madia. In: S. N. Romaniuk, M. S. Catino & C. A. Martin, eds. The Handbook of Homeland Security. s.l.:CRC Press, pp. 187-196.