Damian Czapik, MA
WSB University in Dąbrowa Górnicza
damian.czapik@student.wsb.edu.pl
ORCID 0009-0001-7224-7462

DOI: 10.26410/SF_2/25/4

USING OPEN SOURCE INTELLIGENCE TO COMBAT HYBRID THREATS: REVIEW AND CASE STUDIES

Abstract

In the face of dynamic changes in the security environment and a growing number of hybrid activities, the role of white intelligence (OSINT) in identifying and countering these threats is becoming increasingly important. The article addresses the use of open sources of information in the processes of identifying, detecting, analysing, assessing and documenting activities of a hybrid nature, which may include disinformation, cyber attacks, social manipulation and, consequently, destabilisation of state structures. The definition and characteristics of hybrid threats and white intelligence are presented. In the course of the research, ten case studies of hybrid activities from the period 2013-2023 were analysed. The article concludes with a conclusion on the importance of white intelligence including the role of open sources of information in detecting and combating hybrid activities.

Keywords

Open-source intelligence, OSINT, hybrid threats, the role of information, security, information analysis

Introduction

In the modern world, threats are no longer exclusively in the form of conventional actions. They also take the form of hybrid actions. a threat in which a potential aggressor does not wear a uniform, flags of nationality or other identifying elements poses difficulties in terms of recognition and detection. Such a situation creates space for individual actors, groups of individuals and criminal or terrorist organisations to carry out activities aimed at destabilising public order, weakening state security structures and instilling fear in the public. In a hybrid threat environment, the line between peacetime and armed conflict becomes blurred. Hybrid threats can take various forms of influence including the form of, inter alia, a social media campaign seeking to create information chaos, in parallel with physical acts of terror. For this reason, the use of modern analytical tools, such as white intelligence sources and methods, which allow the identification of potential threats already at the stage of action planning by the adversary, becomes particularly important. Effective analysis of open sources of information is becoming a key element in countering modern hybrid threats.

There are no research studies in the literature that comprehensively address the use of white intelligence in identifying, detecting, analysing, documenting and countering all hybrid threats. One can only come across similar topics relating to the use of white intelligence in the identification of terrorist and cyber threats.

The paper aims to analyse and assess the extent to which white intelligence can become an important tool to identify and respond to hybrid threats. The sub-objectives of the paper include analysing and assessing real-life situations in which information obtained through white intelligence was involved in responding to hybrid threats.

The main research question is: *To what extent can white intelligence be an effective tool in identifying, analysing and countering hybrid threats?* The specific questions to the research question posed are: What forms of hybrid threats have occurred globally between 2013 and 2023? and What practical examples support the effectiveness of using OSINT in counter-hybrid operations?

This thesis is part of the security sciences research strand, particularly in the area of analysis of information security, the use of white intelligence and hybrid threats in the modern world.

An interdisciplinary approach was used to address the adopted research problem. Research methods such as the theoretical method, literature studies and content analysis of accounts and source materials were used in this study. The applied research methods made it possible to formulate conclusions on the role and significance of white intelligence as a tool supporting reconnaissance processes in the context of hybrid threats.

The research analysed ten case studies of hybrid actions from 2013-2023 (including the annexation of Crimea, the downing of flight MH17, Islamic State (IS/ISIS) actions around the world and the migration crisis on the Polish-Belarusian border). Secondary sources were used, including academic publications, reports from international institutions (e.g. Bellingcat, FBI, European Commission), press articles, studies by investigative journalists and social media data. a content analysis of white intelligence material was conducted to identify recurring patterns of counter-hybrid activity. For each incident, the source of the information, how it was used, the actors analysing it and the effect (including identification of perpetrators, international reactions, sanctions) were analysed. The methodological objective was to indicate to what extent white intelligence can act as an early warning tool and decision support in hybrid threat identification processes.

The study is preliminary and serves to initiate a broader discussion on the use of white intelligence in identifying hybrid threats.

White intelligence and hybrid threats

A hybrid threat is a situation in which an adversary (both state and non-state) uses diverse methods of action to achieve its objectives at the strategic level. It is characterised by combining political, military, economic, social and informational means with various forms of aggression, which may include conventional warfare, irregular action, terrorism, diversion or criminal activity[1]. Hybrid threats are defined identically by the European Union, where they are referred to as *a combination of repressive and subversive actions using conventional and unconventional methods (i.e. diplomatic, military, economic and technological) that can be used in a coordinated manner by state and non-state actors to achieve specific objectives, with actions below the threshold of officially declared war*[2]. Hybrid threats occur during hybrid operations resulting in hybrid warfare[3]. Hybrid activities include, but are not limited to: disinformation activities, propaganda activities, cyber-attacks (cyber-attacks), interference in political processes, imposition of economic pressure, instrumentalisation of irregular migration, state support of armed groups and hiring of mercenaries, intelligence operations of a diversionary and sabotage nature, terrorist activities and the use of chemical, biological, radiological and nuclear agents[4].

Due to the increasing complexity and ambiguity of hybrid threats, modern information-gathering methods that allow for their early identification and

1 *Encyklopedia bezpieczeństwa wewnętrznego*, A. Misiuk, J. Itrich-Drabarek, M. Dobwolska-Opała (ed.), Warsaw 2021, p. 295.

2 European Commission, *Joint Framework on countering hybrid threats a European Union response*, European Commission, Brussels 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018, (accessed: 26.06.2025).

3 B. Pacek, P. Pacek, *Psychologia wojny hybrydowej*, Warsaw-Siedlce 2019, p. 11.

4 F. Bryjka, *Rozwój unijnych zdolności do zwalczania zagrożeń hybrydowych*, „Strategic File", 9(117), 2022, p. 2.

counteraction are of particular importance. One important tool in this area is white intelligence, which enables the acquisition of a broad spectrum of information, the analysis of the information environment and the identification of potential threats before they take the form of open aggressive actions.

White intelligence[5] (open source interview) has the task of obtaining information from non-confidential as well as publicly available sources is also called OSINT (Open Source Intelligence). It is defined *as produced from publicly available information that is collected, used and disseminated over a specified period of time to appropriate audiences for specific intelligence needs*[6]. This type of information gathering is based on the use of open source tools[7] mainly obtained through observation or requests for access to information[8]. a hallmark of white intelligence is the obtaining of information using legitimate sources, which can be free as well as those that can be accessed for a fee. There is broad agreement among experts that the effort put into validation, analysis and dissemination in white intelligence distinguishes it from other types of information[9]. In the literature, white intelligence is also divided into passive and active reconnaissance activities[10]. Passive OSINT is observing the world, in this respect there is a lack of integration with the object of observation with whom one does not interact, making one an unobservable person. Active OSINT are activities that seek to interact with the object i.e. befriending the target e.g. commenting on posts to gain more information in an overt manner[11].

Hybrid threats pose a serious danger to the defence system of a state, including mainly its institutions and citizens. The reconnaissance potential of white intelligence is becoming an important means to counter and identify such threats.

Use of white intelligence and response to hybrid threats

White intelligence in responding to hybrid threats can be a significant preventive measure. In the context of reconnaissance and detection activities, OSINT can be used to analyse the flow of information from public media, which can facilitate the identification of the sources of dissemination of false information. It also allows a wide range of post-detection activities to identify the perpetrator. The value of white intelligence is that it can be used as circumstantial and evidentiary material.

5 A. Ziółkowska, *Open Source Intelligence (OSINT) as an element of military recon*, „Security and Defence Quarterly" 19/2, 2018, p. 69.

6 K. Wosiński, *Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu*, Warsaw 2024, p. 11.

7 K. Wosiński, *OSINT: Nowy wymiar poszukiwań w sieci.*, Kraków 2024, p. 11.

8 K. Wosiński, *Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu*, Warsaw 2024, p. 9.

9 D. V. Puyvelde, F. T. Rienzi, *The rise of open-source intelligence*, „European Journal of International Security" 2025, p. 4.

10 B. Terebiński, *OSINT vs. ensuring the security of legally protected information*, „Wiedza Obronna", vol. 287 no. 2/2024, p. 149.

11 D. Meredith, *The OSINT Handbook: a practical guide to gathering and analyzing online information*, 2024, p. 3.

Hybrid action detection is based on the early recognition of symptoms and signals indicating the possibility of threats, which may originate from both foreign states and non-state actors acting on their orders or on their own initiative, who may be motivated by radical views. Hybrid operations are characterised by multilayered and coordinated use of various means of social and informational influence.

In the early stages of detecting hybrid activity, white intelligence enables the collection of data from publicly available sources, which include news portals, social media, discussion forums, video platforms and apps through to public records. This makes it possible to quickly isolate anomalies in news narratives, identify organised disinformation campaigns and identify links between accounts responsible for creating and disseminating this content.

In this case, white intelligence makes it possible:

- a linguistic and semantic analysis of the message, which makes it possible to determine the source and purpose of the message,
- identifying the identities of fake creators and bots used to amplify propaganda messages,
- carrying out monitoring of social trends and sentiments and their background, so that potential escalations of social tensions can be forecast,
- mapping of networks between individuals, institutions and actors involved in content dissemination.

White intelligence can be a key enabler in this process, allowing information to be obtained from open sources in a legal and non-interfering manner. These can be used to augment operational or preventive actions. In the following, I have presented cases of the use of white intelligence in the field of counter-hybrid operations by referring to disclosed hybrid activities widely reported and analysed in the public and academic media.

Sketch 1. Cases of use of white intelligence in counter-hybrid operations

Hybrid threat	Time period	Description of the incident	Use of white intelligence	Effect of action
Terrorist attack during Boston marathon	April 2013	Improvised explosive device (IED) explosion at the finish line of the Boston Marathon. a sectarian terrorist attack carried out by two individuals (jihadists)[12].	Carrying out activities to search for the perpetrators of the attack through the use of amateur photographs and films and the image of likely perpetrators made available to the public[13]. Use of information obtained from social media in the course of an investigation[14].	Identification of the identity of the perpetrators of the attack through the released image of persons at the scene and the ongoing investigation carried out by the Federal Bureau of Investigation. Detention of the person responsible, the other died during the attempted arrest. Increased scrutiny of student visas[15].
The annexation of Crimea by the Russian Federation and the interference of the so-called "green men" on Ukrainian territory.	February/ March 2014	The encroachment on Ukrainian territory of unmarked and unidentified military units, uniformed without distinction or signs of national affiliation. The official narrative of the Russian Federation at the time was that there was no involvement in the conduct of these operations[16].	Carrying out activities in the course of analysing the uniforms and equipment of the attackers, establishing the location of the deployment of persons through metadata of photos and videos disseminated on the Internet. Recognition and identification of participating Russian soldiers on social media[17].	The disclosure that soldiers of the Russian Federation army and its forces and resources were behind the diversionary actions. Russia's hypocritical narrative has been revealed In view of the above, the imposition of sanctions through the European Union against the Russian Federation[18].

12 Państwowa Agencja Prasowa, *Dżochar Carnajew uznany za winnego zamachu w Bostonie*, https://wiadomosci.wp.pl/dzochar-carnajew-uznany-za-winnego-zamachu-w-bostonie-6025268084437633a, (accessed: 14.07.2025).

13 FBI, Boston Marathon Bombing, https://www.fbi.gov/history/famous-cases/boston-marathon-bombing, (accessed: 01.07.2025).

14 K. Wosiński, *O jeden OSINT za daleko, czyli przykre skutki złych analiz [Czwartki z OSINTem]*, https://sekurak.pl/o-jeden-osint-za-daleko-czyli-przykre-skutki-zlych-analiz-czwartki-z-osintem/, (accessed: 01.07.2025).

15 CNN, Skutki zamachu w Bostonie – ostrzejsze kontrole studentów, https://www.wprost.pl/swiat/398399/skutki-zamachu-w-bostonie-ostrzejsze-kontrole-studentow.html, (accessed: 14.07.2025).

16 M. Podraza, *Rosyjska aneksja ukraińskich terytoriów okupo*wanych w świetle prawa międzynarodowego, „Biuletyn Stowarzyszenia Absolwentów i Przyjaciół Wydziału Prawa Katolickiego Uniwersytetu Lubelskiego", t. XVIII, 20(2)/2023, pp. 221-222.

17 I. Ostanin, *Revealed: Around 40 Russian Troops from Pskov Died in the Ukraine, Reinforcement Sent In*, https://www.bellingcat.com/news/mena/2014/08/27/revealed-around-40-russian-troops-from-pskov-died-in-the-ukraine-reinforcement-sent-in, (accessed: 03.07.2025).

18 Rada Unii Europejskiej, Sankcje UE wobec Rosji – kalendarium, https://www.consilium.europa.eu/pl/policies/sanctions-against-russia/timeline-sanctions-against-russia, (accessed: 14.07.2025).

Hybrid threat	Time period	Description of the incident	Use of white intelligence	Effect of action
The downing of Malaysia Airlines flight 17 over Ukrainian territory.	July 2014	Shooting down of Malaysia Airlines plane over Ukraine in Donetsk region by Russians with 9K37 Buk missile launcher[19].	Implementation of activities through analysis of photos, movement of military equipment, testimonies of local residents, entry on Igor Girkin's VK platform[20] and its subsequent removal. Also using posts and videos on social media platforms.	Facts of the downing and the responsibility of the Russian Federation for the downing of the aircraft have been confirmed. Disclosure of this responsibility in investigations and international reports[21]. Imposition of sanctions on the Russian Federation[22].
IS / ISIS (Islamic State), online recruitment, propaganda and terrorist attacks[23].	2014 – 2020	Islamic State (IS/ISIS) propaganda efforts, recruitment of fighters through social media, fundraising and terrorist attacks[24].	Identification and tracking of sources in the form of recruitment channels, accounts and groups. Identification of links of people involved in ISIS recruitment[25]. Determination of geolocation data and identification of their links in the network[26]. Findings of institutions (foundations) supporting ISIS.	Closing down multiple channels of recruitment, foundations, establishing the identity of militants, detaining people linked to the Islamic State.
Russian disinformation campaign interfering in the election.	2016 – 2020	Information campaigns carried out using the method of disseminating disinformation ahead of the US election.	Analysis of metadata and IP sources, bot accounts and users of various platforms, as well as mapping and identifying sources of propaganda and disinformation narratives.	US Senate report revealing the influence structures of the Russian Federation and the influence of trolls (e.g. IRA)[27].

19 E. Higgins, The Buk That C*ould – An Open Source Odyssey*, https://www.bellingcat.com/news/uk-and-europe/2014/07/28/the-buk-that-could-an-open-source-odyssey, (accessed: 04.07.2025).

20 TŁ., Europejski trybunał: Rosja stoi za zestrzeleniem pasażerskiego boeinga, https://www.tvp.info/87748630/katastrofa-samolotu-malaysia-airlines-mh17-europejski-trybunal-praw-czlowieka-etpcz-to-rosja-odpowiada-za-zestrzelenie-pasazerskiego-samolotu-malaysia-airlines-mh17, (accessed: 03.07.2025).

21 A. Holligan, K. Vandy, *MH17: Three guilty as court finds Russia-controlled group downed airliner*, https://www.bbc.com/news/world-europe-63637625, (accessed: 14.07.2025).

22 Council of the European Union, Foreign Affairs Council , 22 July 2014, https://www.consilium.europa.eu/en/meetings/fac/2014/07/22, (accessed: 14.07.2025).

23 O. Reczko, *OSINT – otwarte źródła w walce z z*agrożeniami, https://rynekinformacji.pl/osint-przy-wykrywaniu-zamachowca-w-usa/, (accessed: 04.07.2025).

24 A. Badawy, E. Ferrara, *The Rise of Jihadist Propaganda on Social Networks*, „Journal of Computational Social Science", 2018, p. 11.

25 M. M. Robinson, *Social media recruitment and online propaganda by extremist groups*, University of Northern Iowa 2022, https://scholarworks.uni.edu/cgi/viewcontent.cgi?article=1540&context=hpt, (accessed: 06.07.2025).

26 M. Lakomy, *Internet w działalnośći tzw. Państwa Islamskiego: nowa jakość cyberdżihadyzmu?*, „Studia Politologiczne", 2015, p. 159.

27 *Repor tof the select committee on intelligence United States Senate on russian active measures campaigns and interference in the 2*016 U.S. election volume 2: russia's use of social media with additional views, https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-report-volume2.pdf, (accessed: 08.07.2025).

Hybrid threat	Time period	Description of the incident	Use of white intelligence	Effect of action
Syria to identify responsibility in war crimes committed against civilians.	March/ April 2017	Publication of social media footage of the use of chemical weapons by armed forces against civilians. Activities carried out by the Assad regime The regime of Bashar al-Assad.	Geolocation of video footage, analysis of images of bomb debris and flight trajectories, and drawing on metadata. Analysis of evidence of the occurrence from public and social media.	The results of the investigations provided evidence against the regime of Bashar al-Assad. The Bellingcat organisation (which specialises in OSINT investigations) confirmed the use of SARIN battle gas from the air[28].
Wagner Group in Africa.	2020 – 2023	Support by Wagner Group mercenaries (Russian private military company) of instability and local conflicts in, among others, the Central African Republic, Mali, Sudan and Libya (Sahel and North West Africa Region).	Monitoring the presence of the Wagner group through geolocalisation analyses[29], photographs and films and satellite distribution. Tracing sources and propaganda narratives and links of associated individuals. Documenting crimes and warfare.	Determining in which countries the Wagner Group operates. Identifying commanders, members and their connections. The occurrence of international pressure[30] and sanctions[31].
Rioting and an attack on the US Capitol.	January 2021	Using social media to plan and organise a march on Capitol Hill[32].	Identification of participants and instigators of the riots by analysis of photographs and recordings[33]. Documenting and archiving digital evidence. Use of white intelligence sources as evidence.	Disclosure of identity of rioters. Arrests and indictments following identification of persons[34].

28 E. Higgins, *The OPCW Fact Finding Mission Confirms More Sa*rin and Chlorine Use in Syria, https://www.bellingcat.com/news/mena/2018/06/13/opcw-fact-finding-mission-confirms-sarin-chlorine-use-syria/, (accessed: 08.07.2025).

29 ADDO, Video Stars: Russia's viral video propaganda in Africa, https://disinfo.africa/video-stars-russias-viral-video-propaganda-in-africa-2663403a85f0, (accessed: 16.07.2025).

30 S. Magdy, *US seeks to expel Russian mercenaries from Sudan, Libya*, https://apnews.com/article/russia-ukraine-putin-politics-libya-government-b4218ab0163e6c5e271a3902cd893759, (accessed: 09.07.2025).

31 DW, *EU sanction*s Russian Wagner Group for African operations, https://www.dw.com/en/eu-sanctions-russian-wagner-group-for-african-operations/a-64822435?, (accessed: 09.07.2025).

32 P. Czajkowski, FBI: Atak na Kapitol nie był planowany w mediach społecznościowych. Brak dowodów na udział Trumpa, https://ithardware.pl/aktualnosci/fbi_atak_na_kapitol_nie_byl_planowany_w_mediach_spolecznosciowych_brak_dowodow_na_udzial_trumpa-17533.html, (accessed: 09.07.2025).

33 M. Burgess, Open-source sleuths are already unmasking the Capitol Hil*l mob*, https://www.wired.com/story/capitol-riot-photos-video-online/, (accessed: 10.07.2025).

34 G. Myre, How Online Sleuths Identified Rioters At The Capitol, https://www.npr.org/2021/01/11/955513539/how-online-sleuths-identified-rioters-at-the-capitol, (accessed: 10.07.2025).

Hybrid threat	Time period	Description of the incident	Use of white intelligence	Effect of action
Start of the migration crisis on the Polish-Belarusian border (EU border and Schengen area)	2021	Hybrid actions with the use of migrants on the Polish-Belarusian border. Disinformation and illegal crossing of the Polish State border[35] including the Schengen Area.	Monitoring of foreign accounts, analysis of videos, photos and posts made on social media. Analysis of foreign media information. Analysis of metastasis channels. Verification of disinformation content.	Blocking some of the channels of transit[36], unmasking the disinformation campaign[37], and identifying points of transit and places of concentration of migrants.
Russian Federation's military invasion of Ukrainian territory.	February 2022	Early detection of movements and dislocation of Russian troops prior to invasion. Accumulation of troops near the border from autumn 2021[38] , in the official media coverage under the pretext of a military exercise entitled Zapad-2021.	Analysis of satellite imagery[39], soldiers' posts and video footage and photos on social media. Identification of equipment, equipment and combat units. Mapping of warfare by updating troop movements, frontline maps and equipment losses. Tracking official and unofficial reports on warfare. Identification and documentation of war crimes (e.g. Bucza)[40].	International warning and defence preparedness. Evidence from white intelligence sources was used by NATO member states and the EU as factual evidence of the invasion and war crimes[41].

Source: own elaboration.

The above examples illustrate that white intelligence is widely applicable to hybrid threat operations. It is a valuable tool and source of information. Its application has a bearing on the outcome of hybrid threat operations. OSINT is an important element in recognising, identifying, analysing and documenting such threats.

35 O. Filipec, *Multilevel Analysis of the 2021 Poland-Belarus Border Crisis in the Context of Hybrid Threat*s, „Central European Journal of Politics", Vol. 8(1)/2022, pp. 2–3.

36 M. Scislowska, Y. Karmanau, *Why tensions have been growing along NATO's eastern border with Belarus*, https://apnews.com/article/nato-poland-belarus-wagner-migrants-explainer-aad1f9d81ce9eaed2fed0d6128fa528d, (accessed: 11.07.2025).

37 M. D. Weiss, M. Richter, *How a Manufactured Mi*grant Crisis Showed That Europe's Last Dictator Can Rattle the E.U., https://time.com/6121141/belarus-europe-migrants, (accessed: 11.07.2025).

38 Planet (SkySat), *The Most D*ocumented Invasion In History, www.planet.com/ukraine-photo-story/, (accessed: 17.07.2025).

39 M. Meaker, *High* Above Ukraine, Satellites Get Embroiled in the War, www.wired.com/story/ukraine-russia-satellites/, (accessed: 11.07.2025).

40 E. Higgins, *Russia's Bucha 'Facts' Versus the Evidence*, https://www.bellingcat.com/news/2022/04/04/russias-bucha-facts-versus-the-evidence, (accessed: 17.07.2025).

41 V. Elliott, *The US Plan to Document War Crimes in Ukraine*, www.wired.com/story/conflict-observatory-ukraine-russia-war-crimes/, (accessed: 17.07.2025).

Regardless of the type of hybrid threats present, white intelligence provides the tools and means to:

- responding dynamically to incidents by promptly analysing publicly available material and sources, particularly from social media (e.g. photos, videos, posts, geolocalisation data and metadata) and live streaming services (e.g. YouTube, Snap, Instagram, Twitch). Observation of sources enables correlations of information reliability.
- update and verify information particularly related to crisis situations through real-time tracking of, inter alia, live reports, journalistic coverage, satellite image viewing and social media monitoring, as well as information provided by whistleblowers.
- support decision-making and analytical processes at tactical, operational and also strategic levels,
- secure and familiarise themselves with evidence that can be used in investigative activities and to draw consequences for perpetrators of hybrid activities.

In view of the above, it can be concluded that the development of competencies in the use of white intelligence and the systemic implementation and framing in the field of state security of such tools as part of the practice of recognising, identifying and documenting crime and hybrid threats is applicable.

In order to effectively use white intelligence in the role of identifying and responding to hybrid threats, it is necessary to apply an algorithm of activities, the application of which can translate into effective detection, circumstantial and evidentiary actions.

Sketch 2. Algorithm of white intelligence activities in countering hybrid threats.

Stage of action	Activities with OSINT	Achievable effects
Detection (disclosure)	Monitoring of forums, social media including groups, communities, organisations and public information sources. Analysis of social trends and identification of anomalies. Revealing indications of possible hybrid threats.	This action enables early warning (prevention) and preparation of a response to the possible occurrence of hybrid threats. It also enables a rapid response to threats that already exist.
Hazard analysis (risk assessment)	Threat analysis through visualisation of information sources including identification of links between people, groups, communities, places and things. It enables a comprehensive picture of the situation and the identification of potential threats and better decision-making.	This activity makes it possible to identify external and internal influence structures, analyse the intentions, motives and purpose of the activity including risk levelling. This activity makes it possible to identify key actors and assess the potential impact of their activity on national security.

Stage of action	Activities with OSINT	Achievable effects
Verification of facts (reliability of information)	Confrontation with other sources of information from individuals, institutions, organisations through the public media into the scope which includes open source information. Allows for findings on targeted evidentiary and circumstantial issues. Analysis of the credibility of information and possible threats. Enables verifying the true version of events, identifying discrepancies, and building a coherent and credible picture of the situation.	Act by separating false from true information. Establishing the credibility of information sources and facts. Prioritising action resulting in effective information management. Acting to minimise the risk of disinformation.
Reporting (documenting)	Creation of reports by whistleblowers and reports addressed to national security services. Transmission of verified information. Documenting material by securing it for future evidence or background information.	Action through whistleblowers to support services for targeted action. Enables effective prioritisation of threats and optimisation of the response process. Action by securing digital traces and securing evidence.

Source: own elaboration.

The steps indicated provide a structured model for the use of white intelligence in countering hybrid threats. The application of this algorithm can enable the effectiveness of security services to be increased. The coordinated use of these stages makes it possible to treat white intelligence not only as a tool supporting detection activities and response to hybrid threats, but as a fully-fledged element of the state security system.

Summary

Contemporary hybrid threats, are characterised by multidimensionality and irregularity. It involves the integration of military, informational and psychological activities. White intelligence is gaining importance as a tool with significant action in terms of detection, prevention, analysis and response to such challenges. The examples in the research analysis presented here confirm the effectiveness of this type of action. White intelligence enables the collection of information from open sources, including primarily social media, websites, public records or satellite imagery. The use of this intelligence method results in the possibility to identify perpetrators (including crimes, disinformation and terrorist attacks), influence structures (external and internal) and sources of information distribution. OSINT also makes it possible to secure evidence that can be used in domestic and foreign proceedings.

The area and effectiveness of the use of white intelligence indicates that it should be permanently integrated into the state security system and participate in the

identification and counteraction of hybrid threats. The examples presented in the research paper indicate that the cooperation of services with the public through the exchange of information is significant in order to increase the effectiveness of detection and neutralisation of existing hybrid threats (sharing of images and photographs and recordings seeking to identify the perpetrators). The reliability of open-source information is based on its verification, which has the effect of preventing disinformation, particularly in a changing and computerised environment. The examples shown indicate that white intelligence, through the documentation and archiving of information, has evidentiary as well as operational significance.

An algorithm for countering hybrid threats using white intelligence, based on early detection (disclosure), threat analysis (risk assessment), fact verification (information credibility) and reporting (documentation), provides a structured approach to the use of white intelligence in the practice of whistleblowers and state security services.

Bibliography

ADDO, *Video Stars: Russia's viral video propaganda in Africa*,

https://disinfo.africa/video-stars-russias-viral-video-propaganda-in-africa- 2663403a85f0

Badawy A., Ferrara E., *The Rise of Jihadist Propaganda on Social Networks*, „Journal of Computational Social Science" 2018.

Bryjka F., *Rozwój unijnych zdolności do zwalczania zagrożeń hybrydowych,* „Strategic File", 9(117)/2022.

Burgess M., *Open-source sleuths are already unmasking the Capitol Hill mob*, https://www.wired.com/story/capitol-riot-photos-video-online/.

CNN, *Skutki zamachu w Bostonie – ostrzejsze kontrole studentów*, https://www.wprost.pl/swiat/398399/skutki-zamachu-w-bostonie-ostrzejsze- kontrole-studentow.html.

Council of the European Union, *Foreign Affairs Council*, https://www.consilium.europa.eu/en/meetings/fac/2014/07/22

Czajkowski P., *FBI: Atak na Kapitol nie był planowany w mediach społecznościowych. Brak dowodów na udział Trumpa,* https://ithardware.pl/aktualnosci/fbi_atak_na_kapitol_nie_byl_planowany_w_

mediach_spolecznosciowych_brak_dowodow_na_udzial_trumpa-17533.html

DW, *EU sanctions Russian Wagner Group for African operations*,

https://www.dw.com/en/eu-sanctions-russian-wagner-group-for-african- operations/a-64822435?

Encyklopedia bezpieczeństwa wewnętrznego, Misiuk A., Itrich-Drabarek J., Dobwolska-Opała M. (ed.), Warsaw 2021.

Elliott V., *The US Plan to Document War Crimes in Ukraine*, www.wired.com/story/conflict-observatory-ukraine-russia-war-crimes/

European Commission, *Joint Framework on countering hybrid threats a European Union response*, European Commission, Brussels 2016,

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018.

FBI, *Boston Marathon Bombing*,

https://www.fbi.gov/history/famous-cases/boston-marathon-bombing

Filipec O., *Multilevel Analysis of the 2021 Poland-Belarus Border Crisis in the Context of Hybrid Threat*s, „Central European Journal of Politics", Vol. 8(1)/2022, pp. 1-18.

Higgins E., *Russia's Bucha 'Facts' Versus the Evidence*, https://www.bellingcat.com/news/2022/04/04/russias-bucha-facts-versus-the- evidence

Higgins E., *The Buk That Could – An Open Source Odyssey*, https://www.bellingcat.com/news/uk-and-europe/2014/07/28/the-buk-that-could- an-open-source-odyssey

Higgins E., *The OPCW Fact Finding Mission Confirms More Sarin and Chlorine Use in Syria*, https://www.bellingcat.com/news/mena/2018/06/13/opcw-fact-finding-mission-confirms-sarin-chlorine-use-syria/

Holligan A., Vandy K., *MH17: Three guilty as court finds Russia-controlled group downed airliner*, https://www.bbc.com/news/world-europe-63637625

Kuciel D., *OSINT sztuka zdobywania informacji*, 2023.

Lakomy M., *Internet w działalności tzw. Państwa Islamskiego: nowa jakość cyberdżihadyzmu?*, „Studia Politologiczne", 2015, p.156-184.

Magdy S., *US seeks to expel Russian mercenaries from Sudan, Libya*, https://apnews.com/article/russia-ukraine-putin-politics-libya-government-b4218ab0163e6c5e271a3902cd893759

Meaker M., *High Above Ukraine, Satellites Get Embroiled in the War*, www.wired.com/story/ukraine-russia-satellites/

Meredith D., *The OSINT Handbook: a practical guide to gathering and analyzing online information*, 2024.

Myre G., *How Online Sleuths Identified Rioters At The Capitol*, https://www.npr.org/2021/01/11/955513539/how-online-sleuths-identified-rioters-at-the-capitol

Ostanin I., *Revealed: Around 40 Russian Troops from Pskov Died in the Ukraine*, *Reinforcement Sent In*,

https://www.bellingcat.com/news/mena/2014/08/27/revealed-around-40-russian-troops-from-pskov-died-in-the-ukraine-reinforcement-sent-in

Pacek B., Pacek P., *Psychologia wojny hybrydowej*, Warsaw-Siedlce 2019.

Państwowa Agencja Prasowa, *Dżochar Carnajew uznany za winnego zamachu w Bostonie*, https://wiadomosci.wp.pl/dzochar-carnajew-uznany-za-winnego-zamachu-w-bostonie6025268084437633a

Podraza M., *Rosyjska aneksja ukraińskich terytoriów okupowanych w świetle prawa międzynarodowego*, „Biuletyn Stowarzyszenia Absolwentów i Przyjaciół Wydziału Prawa Katolickiego Uniwersytetu Lubelskiego" t. t. XVIII, 20(2)/2023 pp. 219-233.

Planet (SkySat), *The Most Documented Invasion In History*,

www.planet.com/ukraine-photo-story/

Puyvelde D. V., Rienzi F. T., *The rise of open-source intelligence*, „European Journal of International Security" 2025.

Rada Unii Europejskiej, *Sankcje UE wobec Rosji – kalendarium*, https://www.consilium.europa.eu/pl/policies/sanctions-against-russia/timeline-sanctions-against-russia

Reczko O., *OSINT – otwarte źródła w walce z zagrożeniami*, https://rynekinformacji.pl/osint-przy-wykrywaniu-zamachowca-w-usa/

Report of the select committee on intelligence United States Senate on russian active measures campaigns and interference in the 2016 u.s. election ' volume 2: russia's use of social media with additional views,

https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-report-volume2.pdf

Robinson M.M., *Social media recruitment and online propaganda by extremist groups*, University of Northern Iowa 2022,

https://scholarworks.uni.edu/cgi/viewcontent.cgi?article=1540&context=hpt

Scislowska M., Karmanau Y., *Why tensions have been growing along NATO's eastern border with Belarus*, https://apnews.com/article/nato-poland-belarus-wagner-migrants-explainer-aad1f-9d81ce9eaed2fed0d6128fa528d

Terebiński B., *OSINT vs. ensuring the security of legally protected information*, „Wiedza Obronna", vol. 287 no. 2/2024, p. 142-157.

TŁ., *Europejski trybunał: Rosja stoi za zestrzeleniem pasażerskiego boeinga*, https://www.tvp.info/87748630/katastrofa-samolotu-malaysia-airlines-mh17europejski-trybunal-praw-czlowieka-etpcz-to-rosja-odpowiada-za-zestrzelenie-pasazerskiego-samolotu-malaysia-airlines-mh17

Weiss M.D., Richter M., *How a Manufactured Migrant Crisis Showed That Europe's Last Dictator Can Rattle the E.U*, https://time.com/6121141/belarus-europe-migrants

Wosiński K., *Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu*, Warsaw 2024.

Wosiński K., *O jeden OSINT za daleko, czyli przykre skutki złych analiz [Czwartki z OSINTem]*, https://sekurak.pl/o-jeden-osint-za-daleko-czyli-przykre-skutki-zlych-analiz-czwartki-z-osintem/

Wosiński K., *OSINT: Nowy wymiar poszukiwań w sieci*, Kraków 2024.

Ziółkowska A., *Open Source Intelligence (OSINT) as an element of military recon*, „Security and Defence Quarterly" 19/2, 2018, p. 65-77.

About the Author:

Damian Czapik – master's degree in national security and history at the John Paul II Catholic University of Lublin. Student of the doctoral seminar in the discipline of security sciences at the WSB Academy in Dąbrowa Górnicza. Research interests: the role of information in society, information security, the social and military aspect of military operations, and the use of intelligence methods to ensure security.