DOI: 10.31648/pw.12115

Mirosław Minkina
ORCID: https://orcid.org/0000-0002-2391-314X
University of Siedlce

NEW CHALLENGES TO INTELLIGENCE COMMUNITIES

Abstract: This article deals with the changing situation of intelligence communities. The author explains the main reasons for breaking the monopoly of the state on information. The research was performed from a positivist and post-positivist perspective and it considers the so-called mainstream theories. For its purposes, a system analysis was included as well as references were made to the genesis of the information flow and its use by secret services of different countries. In addition, an in-depth study of the activity of Russian and Chinese special services, with the key facts and methods of their operation in mind, was conducted. The analysis confirmed that the secret, closed and elite world of intelligence is becoming radically democratized. At the same time, investigative journalism and independent investigators, e.g. Bellingcat, are of increasing importance to military intelligence in the current reality of the ongoing invasion of Ukraine.

Keywords: international relations, investigative journalism, intelligence, secret services, Bellingcat, China, mobile information

Introduction

Modern intelligence institutions are slowly beginning to realize that they need to function differently. Various possibilities of access to information for academics, activists and hobbyists have been breaking the monopoly of the state, including state intelligence, on information for some time. Based on satellite data available in cyberspace, it is possible to detect new missile launch sites or other military facilities. They may not be noticed by state intelligence institutions due to the burden of other important tasks or the current demand for information from government institutions. Various commercial satellite data analysis centres that are capable of tracking, in particular, missile tests, movements or concentrations of North Korean troops are being created. However, satellite data are not the only source of publicly available information. There are Internet portals that monitor various events in the world, including aircraft and ship routes. Modern databases are huge. Every day, terabytes of various types of materials are posted on social media sites. Mobile phone users have so much valuable information at their disposal that state intelligence structures did not have in the recent past (Open-source… 2021). Current 3D modelling techniques can determine the appearance of an object that

casts a shadow. In order to obtain more complete knowledge based on incomplete or fragmentary image or sound information, one can use the knowledge of experts, academics, or journalists. In this way, the secret, closed and elite world of intelligence is becoming radically democratized. This trend continues to develop, posing a challenge to governments, transforming the way diplomacy functions and, in a way, eliminating the category of secrecy, which had a special status until now. It is noteworthy that before the Russian aggression against Ukraine, secret intelligence information was used to put pressure on the potential aggressor and to make their intentions publicly know (Gustafson | Lomas | Wagner et al. 2024, 400-419). Secret intelligence information was passed on to Putin and the public in order to stop the aggressor and prevent the outbreak of war.

1. The Role of Investigative Journalism and Social Media

After Eliot Higgins started analysing YouTube videos of weapons used in the Syrian war as a hobby in 2010, he eventually realized that his analysis had a much greater potential. In 2014, he founded the investigative journalism website Bellingcat (Bellingcat 2014). The site, using the work of professional journalists and volunteers who have gathered around it, publishes the results of its investigations. They concern, among other things, crime, armed conflicts, and human rights violations. One of its first significant achievements was the investigation of the shooting down of Malaysia Airlines flight MH17 over Ukraine (Harding 2021). Using video footage of a Russian anti-aircraft missile launcher uploaded to the network by local residents and Google Earth, E. Higgins and a group of enthusiasts identified trees, roads, and buildings that allowed them to determine the location of the launcher. One anonymous blogger identified the launcher's home base by comparing a photo of the missile launcher after it was withdrawn to Russia and found that one missile was missing.

Bellingcat conducted a similar investigation of Iran's downing of a Ukrainian passenger plane in January 2020, which Tehran initially denied. The photos from the crash site showed parts of the plane arranged in a manner similar to that after being hit by an anti-aircraft missile. A video posted online showed a stream of light in the sky, a flash and a sound just before the plane went down, as well as certain objects in the background that are located near the Tehran International Airport. The difference of 11 seconds between the flash in the sky and the sound of the explosion allowed the determination of the distance. Using FlightRadar24, where the plane's transponder signal was visible, left no doubt that the plane was shot down by a surface-to-air missile on its flight path. According to the publicly available collected materials, it turned out that the air defence forces of the Iranian Revolutionary Guard Corps mistook the Ukrainian 737-800 (Flight PS752) for an American missile. The analysis also showed that Iran's air defence was in full

combat readiness and had already fired ballistic missiles at two military facilities in Iraq, where the US troops were stationed, in response to killing General Qasem Soleimani, the commander of the Islamic Revolutionary Guard Corps Special Forces, by a US drone in Baghdad five days earlier (Ukraine Rejects… 2022). In the face of this collected varied evidence, Tehran had to admit that this was not a psychological warfare against Iran, as it had been claiming for some time, but a tragic mistake that had been made.

The Bellingcat team is also investigating the war in Ukraine. The team is particularly interested in war crimes committed by Russian soldiers. The analytical base is publicly available materials: photos and videos posted on social media. As Bellingcat's executive director says: "We are discovering the enormity of war for the first time in our lifetime in a way that is near us and a way that we can see it in social media, and Instagram, and TikTok videos. And the volume of war crimes that we believe we are discovering in our daily work is overwhelming" (McCandless Farmer 2022). The war in Ukraine provides disproportionately more material than previous conflicts. During the civil war in Syria, mainly photographs were available, and there was much less video material. The situation has changed significantly with new social media platforms, especially TikTok, which provides 70% of the evidence on the war in Ukraine collected by Bellingcat. The information from video-sharing platforms was collected even before the invasion of Ukraine in February 2022, when people began posting videos showing tanks on the streets of Russian cities on TikTok. These videos not only showed the build-up of the invasion potential, but also allowed for the identification of individual units, their weapons and equipment. Among other things, Bellingcat was able to identify units that were firing banned cluster munitions from the Russian territory at targets in Ukraine. In some cases, it is possible to monitor Russian units all the way from their departure from their permanent deployment site to the area where they are used in combat.

Bellingcat also uses publicly available materials to expose Russian lies that war crimes in the city of Bucha were committed when Ukrainian forces entered the city after the Russians withdrew. The site's analysts verified an aerial video taken by Ukrainian military personnel on March 3, 2022, when Russian troops occupied Bucha. The video shows a woman walking a bicycle along a street where a Russian tank is located. As the woman turns round the corner of the street, she is killed by a shot from the tank. Another video, taken by Ukrainian soldiers in late March and verified by the site, shows the woman's body at the site where she was shot. In this context, it is significant that Ukrainian troops entered Bucha in early April (Higgins 2022). It is worth noting that atrocities committed by the Russian army also took place in other occupied cities, including Kherson and Irpin (Wojna w Ukrainie… 2022).

As a result, in mid-March, the Russian Prosecutor General blocked access to the portal (Bellingcat is Banned… 2022), and through the press officer Dmitry Peskov, the journalistic investigation responded in a brazen Russian manner that "In general, the information of Bellingcat must be perceived through special filters: sometimes with a sense of humour, and sometimes as a deliberate lie and distortion of reality" (McCandless Farmer 2022).

We cannot determine to what extent state intelligence uses information from social networks. However, it can be stated with near certainty that it is significant. At the same time, however, these institutions, influenced by the culture of secrecy (often rightly, but sometimes wrongly), are reluctant to admit this openly. There is also a tendency for information on social media to become the basis for making important political decisions at the state level. This is evidenced, for example, by the request of the US House of Representatives Committee on Oversight and Foreign Affairs to the CEOs of social media portals Meta, Twitter, YouTube and TikTok to archive materials posted on their platforms that could be evidence in courts, in trials for war crimes and human rights violations committed in Ukraine (Oversight and Foreign… 2022)[1].

Intelligence services have always been involved in information warfare, including the production and dissemination of content that is convenient for their own country and harmful to another country, most often an adversary. Russia's aggression against Ukraine has radically changed the way of thinking about the possibilities of using cyberspace, by both Ukrainian society and the authorities. The vast amount of materials posted on the Internet has made Ukraine the most "networked" country ever to be attacked. It has become a clear example of how social media have changed the way a war is documented and the war itself[2]. Posts, comments and audio-visual materials posted on the Internet often become the main source of information for the entities collecting them, including state institutions and traditional media. Some argue that social media have also become an instrument in the hands of the government, used to achieve political and military goals. They are used to exert pressure on economic entities that have not joined the sanctions and to combat Russian disinformation (The Invasion… 2022). Ukrainian public relations specialists have been able to engage broad public circles in information warfare. One of the Ukrainian government advisers claims that they have managed

[1] It is worth marking that according to the latest information, the USA has withdrawn from the group investigating Russian responsibility for the invasion of Ukraine. The latest decision of the Trump administration, as the New York Times reports, is to move away from holding President Vladimir V. Putin of Russia accountable for crimes committed against the Ukrainians (U.S. to Withdraw… 2025).

[2] Ukraine is not an example of the first war on social media. Previous cases include, among others: the conflict between Hamas and Israel, the Russian aggression against Ukraine in 2014-2015, and the conflict between Armenia and Azerbaijan over Nagorno-Karabakh in 2020. However, these events were not covered on the same scale as the current war in Ukraine.

to achieve a situation where every citizen has become an information war fighter. The government has created and coordinated several specialized information warfare groups. One of the groups develops materials aimed at Russians, another one produces patriotic clips for its own society, the third one focuses on TikTok activity, the fourth one produces memes, and yet another one archives photo, audio and video materials from social media for future use as evidence in criminal and war crimes trials (The Invasion… 2022). Through such a system, Ukraine achieves a very important goal: information about Ukraine comes from Ukraine.

2. Offensive Intelligence of the People's Republic of China

In the most general sense, the community of the conventional West must face the intelligence and counterintelligence challenges of two countries: the People's Republic of China and the Russian Federation. Russian intelligence activities are carried out by the Foreign Intelligence Service, the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (formerly the Main Intelligence Directorate, GRU) and the Federal Security Service, which conducts both intelligence and counterintelligence activities. Counteracting the operations of these institutions has not lost its importance, and in the context of the war in Ukraine, it deserves a special attention[3]. Considering the specific role of the FSB in the war against Ukraine, for the occupied regions, in practice, this means the NKVD model of operation: tortures, interrogations, filtration of detainees, and political control over the occupied territory (Soldatov | Borogan 2022).

Regardless of the intelligence threats from Russia, China remains a priority for Western intelligence and counterintelligence services. This approach is evidenced by the statement of the Director of British Intelligence MI6, who claims: "Adapting to a world affected by the rise of China is the single greatest priority for MI6" (Britain's Chief… 2021). Chinese intelligence has efficient staff, who conduct intelligence operations on a large scale. It monitors and harasses the Chinese diaspora, widely using social media and setting the tone of public discourse on various issues. China is expanding its network of authoritarian control around the world through the export of surveillance technology. This is a problem not only for economic entities purchasing Chinese information technologies, but also for Western security institutions. China controls smartphones, apps, telecommunications networks, as well as access to various types of repository of personal information, together with biometric data, including genetic data at the disposal of airports. Such knowledge poses a threat to intelligence institutions, whose officers operating undercover risk being exposed. According to US counterintelligence, China

[3] See more: Minkina 2023.

is expanding its influence in the United States to create a favourable political climate for Chinese business and foreign policy. They are trying to influence politicians and administration officials whose views are incompatible with China's interests (Chinese Political… 2022). One example is the actions taken against a Chinese immigrant, a US citizen, who was running for the Congress in New York. China did not want him to be elected because he had participated in the Tiananmen Square protests. For this purpose, they hired a private detective to find compromising materials on the candidate. When nothing compromising was found, they decided to use a prostitute and cause a car accident (Corera 2022a).

Concerns about interference in political life have also been raised by, among others, Canada and Australia. In a report on the intelligence threat to the state, the Canadian Security Intelligence Service noted a qualitative and quantitative increase in state-sponsored activity related to election interference and the influence of the members of parliament. The report points out two countries: China and Russia. Interference in elections was also noted by the Australian counterintelligence, the Australian Security Intelligence Organisation (Corera 2022a).

A close analysis of these cases shows that the operations to influence political decisions in Western countries are carried out and coordinated by one of the departments of the central apparatus of the Communist Party of China, the United Front Work Department (UFWD). In terms of external activities, the main task of this department is to identify and cultivate people who can promote the goals and tasks of the Communist Party, at the same time opposing and neutralizing those who oppose China's policies and interests in various ways (Foreign Interference… 2020). In practice, this institution focuses its efforts on people of the Chinese nationality who are supposed to establish contacts and build ties between the Communist Party of China and Western intellectual elites and politicians. However, the department also carries out tasks that involve influencing Chinese elites and influential people, i.e. businesspersons, scholars, and religious leaders, in order to persuade them to support state policies and to promote them. A significant part of the resources is directed to work with the elites of Hong Kong and Taiwan.

The functioning of this institution is illustrated by Christine Lee. She did not hide the fact that she was employed as a legal adviser to the Overseas Chinese Affairs Office in the UK, which is a structure of the United Front Works Department (UFWD). She was also the director of the China Overseas Friendship Association, supervised by UFWD (Corera 2022b). She did not hide her connections with the mentioned party institutions, nor the tasks assigned to her by the Chinese leadership. According to the British security services, over the course of several years she transferred the amount of £500,000 to one of the influential MPs from the Labour Party.

Western security services, including the FBI and MI5, agree that China poses the greatest long-term threat to economies and national security. Then-FBI Director

Christopher Wray and then-MI5 Director Ken McCallum met at MI5 headquarters in London in July 2022 to share their concerns and warnings about China with the public. The audience included representatives of business, research centres and universities. The MI5 Director claimed that over the previous three years, the service he headed had devoted more than twice as much effort and resources to counteracting and monitoring Chinese intelligence activities. Compared to 2018, the British security service is conducting seven times more investigations and proceedings related to the activities of various Chinese entities. According to both directors, China poses a much greater threat to Western business than one might expect. This activity is mainly focused on the theft of technology, research results and the recruitment of representatives of scientific and research centres to cooperate. The directors of the services gave examples of the recruitment of experts, including a British specialist in aviation technology. Chinese intelligence offered him a job online and invited him to visit the country. During his stay in China, the expert was very lavishly received, but at the same time, he was asked about the technological details of the military aircraft that the invited specialist had to deal with (Corera 2022a).

In terms of cyber espionage, the Chinese are using the "cheat and steal" method on a massive scale, using more advanced hacking programs than those possessed by some countries. The UK Security Service shares intelligence information on cyber security with 37 countries. This cooperation has helped to prevent the threat of hacking attacks in cyberspace. It is worth noting that China is closely monitoring the armed conflict in Ukraine. Of particular interest is the extent of the Western support for Ukraine in terms of arms supplies and financial assistance on the one hand, and the effects of economic and personal sanctions on the other hand (Corera 2022a). The conclusions from this observation are most likely used to build scenarios for an invasion of Taiwan, in a so-far unspecified perspective.

Beijing's growing military potential and increasingly clear signals regarding the solution of the Taiwan problem, the annexation of the island to the People's Republic of China, have become a serious threat to the global stability and peace. The actions of the Chinese Communist Party, which are destroying the democratic system in Hong Kong, lead to the certainty that, in the event of the annexation of Taiwan, the proclaimed principle of "one country, two systems" will not be respected. Observing the Chinese policy, it is known that this authoritarian state does not tolerate opposition, different opinions and does not respect human rights, which can be seen in the example of the million-strong Muslim community (A Long-awaited… 2022). It is disturbing that China is beginning to believe in its own propaganda, which belittles and devalues the political and military potential of the West. China has shown a certain ignorance of the power of the West by flexing its muscles and simulating an invasion of Taiwan after the visit of the Speaker of the US House of Representatives Nancy Pelosi to the island (How the Crisis… 2022).

China's network of authoritarian control extends to many countries, partly as a result of the export of information technology. Western intelligence services must therefore do more than just detect, understand and anticipate China's actions. In a world where everyone is under the surveillance of electronic devices, in a world of social media and the transfer of personal information during air travel, and financial transactions carried out in cyberspace, intelligence services must develop a methodology for their operations that will be secret and impossible to detect. Perhaps, one way to achieve such a modus operandi is the previously mentioned concept of opening up intelligence services. Covert actions are necessary, for example, to detect and prevent the use of personal, government and economic data. The entanglement of states in debt traps in order to exert pressure on political decisions can be covertly detected.

The activities of the Chinese services are mainly focused on hacking operations and harassing dissidents. In recent years, they have also developed technology theft operations, especially in the areas of robotics, astronautics, and biotechnology. They have also visibly increased the potential of human intelligence. The US Federal Bureau of Investigation estimates that, on average, it opens Chinese espionage cases every 12 hours (China's Spies… 2022). Chinese counterintelligence also functions efficiently, and, as a result of its activities, many American personal sources in China have been sentenced to prison or executed. Chinese intelligence had its own agency in the CIA. In August and November 2020, two former officers of this institution were convicted of spying for China. One of them contributed to the death sentences or imprisonment of 20 CIA informants. In the past, at least four American intelligence officers working for China were identified and convicted (For the First Time… 2021). However, there are opinions that Chinese intelligence services are not as professional and effective as they seem. In a certain sense, Beijing has become a victim of its own intelligence activities. Over the past three decades, they have developed their interests so widely that intelligence institutions have difficulty identifying priorities for information needs. Chinese intelligence, focusing on defence and technology, does not have sufficient potential to penetrate the decision-making process in the capitals of the countries of intelligence interest. The weak link in Chinese intelligence is information analysis. This is due to the hierarchical Chinese culture, which does not allow for the evaluation of acquired materials by lower and mid-level officers. This right is reserved for officials from the level of vice minister and above. Even then, some information will not reach President Xi, when it is not consistent with his views and perception of international reality. Chinese operational officers, unlike the Western ones, often ask their personal sources for written analyses, protecting themselves from personal responsibility for the interpretation of events they convey. Chinese intelligence also avoids the risk of recruiting high-value targets, including people at the top of the political and government systems, choosing easier, less significant targets,

such as retired officials of the ministries of foreign affairs and defence, as well as representatives of the academic world (China's Spies… 2022). American experts and former intelligence officers point out the low level of professionalism of the operational officers recruiting and running the agent. Based on a study that analysed 595 cases of Chinese espionage, it turned out that in 218 cases there was a visible lack of professionalism, including the violation of conspiracy rules (China's Spies… 2022). The case of the expulsion from Afghanistan in 2021 of a dozen people suspected of spying for China is cited as evidence (China 'Unaware'… 2021). Operations against Russia are a challenge to Chinese intelligence. Despite some successes in recruiting Russian sources, China has less insight into the Kremlin's policy (China's Spies… 2022) than Western intelligence, which conducted operations against the Soviet Union for years.

3. Secret Intelligence in the Age of Mobile Information

The changing nature of contemporary threats requires, paradoxically, a greater degree of openness and sharing of their achievements from intelligence institutions. This paradox creates yet another situation that defies the traditional understanding of intelligence as a secret state institution. As Richard Moore, the head of the British Secret Intelligence Service, says, "to stay secret, we are going to have to become more open" (Moore 2022). Intelligence, similarly to entire societies and their institutions, operates in a world that has been revolutionised by ubiquitous digital connections. At the same time, however, we are witnessing the continuous development of information technology, which is transforming our everyday lives and our work in ways that we cannot fully predict. Scientific and technical progress is rapidly changing the production and distribution of material goods. The vast amount of data available in the world and the growing power of computers are rapidly leading to the development and expansion of artificial intelligence into almost every area of our everyday lives. At present, we cannot predict what the consequences will be. It is estimated that we will see more technological advances in the next ten years than in the entire last century. This advancement is beneficial, but it also creates and increases the likelihood of digital attacks by terrorists, criminals, and hostile states.

Therefore, the leadership of each country faces the need to transform and modernize their intelligence institutions. Despite computerization, alongside with technically enabled information gathering and analysis, human intelligence remains a vital instrument in the hands of security institutions and states. However, human intelligence should adapt its work methods and skills to the modern digital age, and it must do so at a much faster pace and in a more innovative way than its opponents. Intelligence agencies will continue to recruit agents from states or non-state entities

that are of interest for cooperation. States will continue to need information about the intentions, plans, methods, motives and mindsets of people making decisions or influencing decisions in the states of the opponent and intelligence interest. Human intelligence is still important because the vast majority of decisions are made by humans. Therefore, there is information important to the state that can only be obtained from an agent recruited for cooperation. Having professional human intelligence also allows us to reduce the space in which the adversary believes that they can act with impunity, online or offline, against our security and our interests.

As mentioned earlier, China has become the most important challenge to all Western and other intelligence agencies as an assertive and constantly growing power. The security and prosperity of many countries in the Euro-Atlantic area are linked to the Chinese activity and policy. Many areas of socio-political reality require relations with China. These include: trade, investments, cultural and scientific ties, as well as global challenges the humanity is facing: climate change and biodiversity. Despite these objective conditions, China is an authoritarian state, professing completely different values than the Western civilization circle. Thus, we are dealing with a situation where Chinese threats coexist with opportunities and the need for cooperation. In this context, Chinese special services conduct large-scale intelligence operations against the West. Making extensive use of their diaspora, they focus their intelligence interests on government administration institutions, political and social system institutions, industry as well as scientific and research centres. In an attempt to influence public discourse and decision-making, Beijing's intelligence services exploit the openness of Western societies, including social media, to carry out their operations. These activities are global in their scope.

Iran has been and has remained a serious challenge to the Western community. This country uses tactics to sabotage any attempts to establish democratic principles and respect for the law in the countries of the region by sponsoring armed gangs and killing law-abiding people. Iran has also created a significant cyber potential, which it uses to fight its rivals in the region, as well as against the countries of Europe and North America. We see many similarities here with Russia's actions. Therefore, it is not surprising that these countries are closely cooperating with each other (Foroutan 2022). Iran's nuclear program is, and will probably continue to be, a serious problem (An Unenriching… 2022).

International terrorism continues to pose a serious challenge to intelligence and counterintelligence services. In order to eliminate terrorist groups and prevent their spread, it is necessary to recruit agents in the most dangerous and conspiratorial organizations. Building human intelligence structures must be supported by the use of modern technologies. Counter-terrorism operations in a divided world, engulfed by conflicts and the poverty resulting from these conflicts, are becoming a complex task, especially since mass access to information technologies, including social networking sites, makes it easier for terrorists to communicate and conceal their intentions.

Conclusions

Obtaining information in the contemporary world of modern technologies, disorder, and high unpredictability of entities operating in the international environment has lost its certain mysticism that was contributed to by the vastness of sources. Therefore, there is a high probability that unreliable information will constitute the basis for making a decision that may turn out to be wrong. Conversely, ignoring information that seems untrue may have consequences in the form of fatal neglect.

Despite the quantitative and qualitative changes in the information environment, intelligence institutions continue to recruit classic agents, agents of influence, conduct observations, eavesdrop, and conduct non-information operations aimed at influencing reality in countries. It is difficult to imagine secret intelligence institutions deprived of the tasks related to supporting foreign policy, including traditional diplomacy (Gentry 2021, 432) or monitoring international treaties and agreements. It seems that warning of aggression and deterrence through the provision of intelligence data will become a more common method of using intelligence information (Massicot 2023, 78-79).

References

A Long-awaited… (2022), A Long-awaited UN Report Condemns China's Actions in Xinjiang, [in:] The Economist 01.09.

An Unenriching… (2022), An Unenriching Debate, [in:] The Economist 10.09.

Bellingcat, [in:] https://www.bellingcat.com/ (accessed: 22.02.2025).

Bellingcat is Banned… (2022), Bellingcat is Banned in Russia. Here's How to Beat the Block, [in:] Bellingcat https://www.bellingcat.com/resources/2022/04/22/how-to-beat-russias-block-on-bellingcat/ (accessed: 26.06.2022).

Britain's Chief… (2021), Britain's Chief Spooks Sees China As the Main Intelligence Threat, [in:] The Economist 04.12, [in:] https://www.economist.com/britain/2021/12/04/britains-chief-spook-sees-china-as-the-main-intelligence-threat (accessed: 28.06.2022).

China 'Unaware'… (2021), China 'Unaware' of Any Afghan Deportation of Chinese on Spying Charges, [in:] Reuters 07.01, [in:] https://www.reuters.com/article/us-afghanistan-china-arrests-idUSKBN29C25U (accessed: 15.09.2022).

China's Spies… (2022), China's Spies Are not Always As Good As Advertised, [in:] The Economist 14.06.

Chinese Political… (2022), Chinese Political Interference Has Western Spooks Worried, [in:] The Economist 21.04, [in:] https://www.economist.com/china/2022/04/21/chinese-political-interference-has-western-spooks-worried (accessed: 18.09.2022).

Corera, G. (2022a), China: MI5 and FBI heads warn of 'immense' threat, [in:] BBC News 07.07, [in:] https://www.bbc.com/news/world-asia-china-62064506 (accessed: 09.09.2022).

Corera, G. (2022b), Why did MI5 name Christine Lee as an 'agent of influence'?, [in:] BBC News 19.07, [in:] https://www.bbc.com/news/uk-62179004 (accessed: 08.09.2022).

For the First Time… (2021), For the First Time, a Career Diplomat Is to Lead the CIA, [in:] The Economist 11.01.

Foreign Interference… (2020), Foreign Interference – China's Use of the United Front Work Department, [in:] Public Safety Canada 9.06, [in:] https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20200930/015/index-en.aspx (accessed: 08.09.2022).

Foroutan, F. (2022), Suspicious Bind: Iran's Relationship with Russia, [in:] European Council on Foreign Relations, [in:] https://ecfr.eu/article/suspicious-bind-irans-relationship-with-russia/ (accessed: 12.09.2022).

Gentry, J. A. (2021), Diplomatic Spying: How Useful Is It?, [in:] International Journal of Intelligence and Counterintelligence 34 (3), 432-462.

Gustafson, K. | Lomas, D. | Wagner, S. et al. (2024), Intelligence warning in the Ukraine war, Autumn 2021 – Summer 2022, [in:] Intelligence and National Security 39 (3), 400-419.

Harding, L. (2021), We Are Bellingcat: The Reinvention of Reporting for the Internet Age, [in:] The Guardian 01.02, [in:] https://www.theguardian.com/books/2021/feb/01/we-are-bellingcat-by-eliot-higgins-review-the-reinvention-of-reporting-for-the-internet-age (accessed: 23.06.2022).

Higgins, E. (2022), Russia's Bucha 'Facts' Versus the Evidence, [in:] Bellingcat 04.04, [in:] https://www.bellingcat.com/news/2022/04/04/russias-bucha-facts-versus-the-evidence/ (accessed: 26.06.2022).

How the Crisis… (2022), How the Crisis over Taiwan Will Change US-China Relations, [in:] The Economist 11.08.

Massicot, D. (2023), What Russia Got Wrong: Can Moscow Learn From Its Failures in Ukraine?, [in:] Foreign Affairs 102 (2), 78-79.

McCandless Farmer, B. (2022), How Bellingcat is Using TikTok to Investigate the War in Ukraine, [in:] CBS News 15.05, [in:] https://www.cbsnews.com/news/bellingcat-tiktok-ukraine-60-minutes-2022-05-15/ (accessed: 26.06.2022).

Minkina, M. (2023), Russian Secret Services in the So-called Special Operation in Ukraine, [in:] Przegląd Wschodnioeuropejski XIV/2, 125-138.

Moore, R. (2022), Speech by SIS Chief Richard Moore: Human Intelligence in the Digital Age, [in:] https://www.sis.gov.uk/richard-moore-first-public-speech.html (accessed: 9.09.2022).

Open-source… (2021), Open-source intelligence challenges state monopolies on information, [in:] The Economist 07.08.

Oversight and Foreign… (2022), Oversight and Foreign Affairs Committees Call on Social Media Companies to Preserve Evidence of Possible War Crimes in Ukraine, [in:] https://oversight.house.gov/news/press-releases/oversight-and-foreign-affairs-committees-call-on-social-media-companies-to (accessed: 26.06.2022)

Soldatov, A. | Borogan, I. (2022), Kak voyennyyemesyatsy izmenili FSB, [Солдатов, А. | Бороган, И. (2022), Как военные месяцы изменили ФСБ,] agentura.ru, [in:] https://agentura.ru/investigations/kak-pervye-voennye-mesjacy-izmenili-fsb/ 2022 (accessed: 08.12.2022).

The Invasion… (2022), The Invasion of Ukraine Is not the First Social Media War, but It Is the Most Viral, [in:] The Economist 02.04.

Ukraine Rejects… (2022), Ukraine Rejects Iran's Final Report on Downing of Flight PS752, [in:] BBC News 17.03, [in:] https://www.bbc.com/news/world-middle-east-56428698 (accessed: 25.06.2022).

U.S. to Withdraw… (2025), U.S. to Withdraw From Group Investigating Responsibility for Ukraine Invasion, [in:] The New York Times 17.03, [in:] https://www.nytimes.com/2025/03/17/us/politics/trump-ukraine-invasion-accountability.html (accessed: 02.03.2025).

Wojna w Ukrainie… (2022), Wojna w Ukrainie. Są kolejne dowody na ludobójstwo. Zniszczone, zaminowane miasta i wsie, trupy na ulicach, [in:] Polska Agencja Prasowa 05.04, [in:] https://www.pap.pl/aktualnosci/news%2C1145757%2Cwojna-w-ukrainie-sa-kolejne-dowody-na-ludobojstwo-zniszczone-zaminowane (accessed: 23.02.2025).