UDC 355.40:004.82(477)   https://doi.org/10.33099/2304-2745/2024-3-82/13-16

V. Kachanov   (0009-0000-8313-3252)

Department of Euro-Atlantic integration and International Peacekeeping Operations, National Defence University of Ukraine, Kyiv

Intelligence, surveillance and reconnaissance

Resume. The article helps to understand the functions, implications, and changes in Intelligence, Surveillance and Reconnaissance (ISR) following the russian full scale invasion in February 2022, how ISR declassification and expedited dissemination provided crucial information for alerting the international community to russia's intent to invade Ukraine and how innovation and adaptation in ISR is being employed during the first year of full-scale Russia-Ukraine War.

Keywords: intelligence, surveillance and reconnaissance, disclosure of information, dissemination of information, false flag operations, Open Source Intelligence (OSINT).

As military experts say intelligence revolution is taking place in the war in Ukraine. Prior to the russian full scale invasion, the US government opened secret information about possible future full-scale russian invasion in Ukraine, including possible russian axes of advance and possible start date of the invasion. The US government initiated the dissemination of this information through mass and social media in order to warn the international community about russia's intent to invade Ukraine. Additionally, commercial assets including satellites, mass and social media, not previously used in warfare, were employed to support open-source intelligence, and are playing an incredibly important role [1, 2].

On 18 February 2022, at a press conference just six days before russian full-scale invasion of Ukraine, the President of the USA Biden stated that he was sure that Putin had made the decision to invade Ukraine. In addition, on 23 February, the day before Russia started its invasion, US Secretary of State Antony Blinken stated that "...Russia will begin its invasion tomorrow" [2].

These series of the US administration statements have some implications. One of them highlighted that the United States possess incredibly serious intelligence capability and this fact helped to identify the date of the start of the russian invasion. Information about russian troops deployment was not too difficult to detect by employing images from satellites and information from different intelligence assets. However, determining the exact timing of an invasion is difficult to convey to other countries' leaders without specific evidence. Second, this intelligence, which is usually to be kept strictly secret from the audience, was made public at the press conference, despite the fact that it would put the source of the information in danger [2].

There were three main reasons for the Biden administration to disclose information [2]. The first was to deter war, and the US Government has released a series of statements revealing secret information. It was hope that publishing this information force the aggressor at least to postpone its plans. Unfortunately, it did not happen and Russia started the war. The second aim was to unite the international community. Initially, however, some NATO leaders and many experts did not believe in possibility of full-scale war in the center of Europe in the 21-st century [2]. In order to change the situation, the US administration made the intelligence about russian possible future aggression available to the international community and this helped to unite different democracies all over the world in its support for Ukraine. As a result, just before the war broke out, strong economic sanctions were imposed on Russia, neighboring countries opened their borders, accepted Ukrainian asylum seekers, and provided all necessary material assistance to Ukraine. The third aim was to counter false information made by Russia. In 2014-th Russia used information operations and produced a serious of false statements temporarily occupied Crimea. And, unfortunately, international support of Ukraine at that time was not so strong, partly because of the impact of russian's information operations. However, in 2022, due to declassification of secret information and its dissemination by different western media, russia's false narrative was largely disregarded by the international community [2].

Alongside with intelligence declassification, open source was incredibly important for intelligence, but it was more important for broader understanding what was going on and as a result improved intelligence making and decision making [2]. Some military

experts stated that the russian-Ukrainian war is the first war where commercially available services and digital capabilities played so important role as traditional military capabilities. Employment of commercial satellites has significantly improved situational awareness on the battlefield and increased speed of action [2]. Besides that, utilization of artificial intelligence alongside with commercial software applications helped to increase the speed of action and utility as well. It has become incredibly important to sense and understand the environment, to decide and act, and then to learn the lessons and adapt. And what is more important – to implement all the lessons learned. So, it is vital to be able to act with sufficient pace in order to outpace the adversary and win.

Open source has had serious impact on intelligence [2]:

the first is the impact on anticipatory intelligence. How we understood the russian military forces build up around Ukraine and the dissemination of commercial satellites images, data and social media analysis, provided situational awareness of deployments. The importance of anticipatory intelligence has played very important role not just for the military, but for public too – in order to understand what was going on. Shifting public confidence, ability to share information about russian activity helped the US administration to unite international partners prior the russian aggression;

countering russia's Information Operations around the war during russian pre-war deployment and revealing russia's intent to international community was important, but also open source has been incredibly important in order to be able to counter russia's false flag operations;

open-source information was also a force multiplier. Through open-source information every platform and every person were able to act as a sensor. Almost every citizen and every mobile phone has become a sensor;

crowdsourcing and the use of standardized chatbots has allowed Ukrainian citizens to report about russian units' locations and movement;

lifting the fog of war: open source gives an almost infinite number of jigsaw pieces and helped to reach greater understanding as a consequence.

Open-source information offers an opportunity to realize what is happening, where it happening, when it happening. It helped to improve situational awareness on the battlefield significantly [2].

Alongside with open-source intelligence, commercial assets such as satellites and social media, has also played an important role [2, 3].

Here some examples:

In mid-February, before the beginning of the full-scale invasion, Russia falsely stated that it had started withdrawing its troops from the Ukrainian borders. In order to reveal russia's false narratives, the Secretary General of NATO demonstrated commercial satellite images and proved that russia's statement was false [2,3]. Mass media available to wide audience, played an important role even before the development of commercial satellites and social media, but in the war in Ukraine, such open-source intelligence plays a new and different role from previous wars [2]. At the end of March 2022, when Ukrainian forces retook the Ukrainian city of Bucha, the international community was shocked when a large number of civilian bodies and mass graves were identified. Russia claimed that this was a Ukrainian fabrication. In response, Western media used commercial satellite images to prove that the bodies lying in the streets of Bucha and the mass graves occurred during russian military occupation of city [4].

Ukraine has also created a mechanism for Ukrainian citizens to provide information to the government using an official app. The app has reportedly been used by many Ukrainian citizens to provide the Government with evidence of russian military movements and war crimes. Ukraine government publishes this information on its website and provides evidence of russian military atrocities to the international community [2, 5].

Ukrainians have also actively donated commercial satellite images for improving situational awareness on the battlefield and conducting strikes on enemy targets. In the middle of fall of 2023 one of Ukraine's volunteer fund, bought the rights for getting images from Finnish commercial satellite ICEYE, which helped to improve detection of enemy forces and its armament location [6].

It is worth to stress that during the first year of full-scale invasion russia's approach of their ISR' employment was not aligned with their doctrines. For instance, russian Special Operation Forces (SOF) mostly have not conducted Strategic reconnaissance actions and Special reconnaissance (Direct) actions due to the fact that they were deployed mostly as part of front-line infantry formations and conducted assaults. [5, 7]. Typically, SOF personnel are assigned the sorts of stealthy, high-risk missions in deep enemy's rear and russia's SOF were not ready to

participate in engagements on the frontline, which led to an extremely high level of casualties among these units [5, 7, 8].

Russia also faced a serious problem with conducting reconnaissance on tactical level. The main reason for that was that Russia had their organic separate reconnaissance battalion and UAVs company in mechanized rifle brigades, but they did not get any reconnaissance assets at the battalion level [5, 7, 8].

As a result, russian military commanders reinforced mechanized rifle battalions with reconnaissance platoons from separate reconnaissance battalions, that is why they had difficulties with interoperability. But Russia tried to improve the composition (structure) of mechanized rifle battalions in order to have an organic reconnaissance asset at the battalion level. Another problem with reconnaissance at the tactical level was the way Russia generated Battalion Tactical Groups or BTGs. BTG – was an ad-hoc formation, created for specific purposes and for set period of time, that is why battalion commanders had limited knowledge about their subordinate reconnaissance units and could not employ them properly. They often used them as an assault unit, and as a result of such decisions reconnaissance units suffered from heavy casualties [5, 7].

Next problem was that russian BTGs suffered from heavy losses and were not able to carry out tasks they were assigned to. So, russian military leaders "solved the problem" – they decided to generate a new BTGs combining two, which had losses in the actions. And according to russian military theorists – the new amalgamated formation with requisite combat power was created. But it did not work because mechanized infantry companies might be from one BTG, but reconnaissance platoon from the other [8, 9, 10]. They were generated from different russian military formations and even from different military districts, that is why the problem with interoperability occurred (different means of communication, encryption keys, logistics and so on) [5, 7, 8].

So, first year of full-scale russian invasion revealed some of the weaknesses of russian Battalion Tactical Groups' ISR [5, 7, 8]:

Inexperienced commanders on battalion level were not able to use ISR assets properly;

Poor training on communication equipment;

Lack of junior leadership;

Confusion as to the location of units;

BTGs' relatively small allocation of combat infantry led to employing reconnaissance units as frontline infantry.

So, one of the lessons learned from russia's way of employing reconnaissance units was that russian force generation was not aligned with its doctrinal concept of operations.

Weaknesses of russian reconnaissance units and problems on the battlefield forced russians to employ disposable infantry in addition to ISR assets [9, 10]. Disposable Infantry was mostly used on most dangerous axis of advance in front of organic russian mechanized units and employed human waves tactics and disposable fire teams (up to 5 personnel) – usually mobilized from temporarily occupied Luhansk and Donetsk Regions (heavily attired from early rounds of fighting), prisoners drafted by the Wagner group and under-trained mobilized russian civilians.

Wagner group tactics was based on the concept of human waves [5]. They formed assault groups from 8-10 up to 30-50 personnel in each one. Their task was to approach to Ukraine Defence Forces' positions as close as possible, using arms and grenades, and capture a trench under the cover of fire of automatic grenade launcher AGS-17 Plamya. Tanks and IFVs were not usually used for fire support in order to avoid counterbattery fire. Leaders of each assault group had a tablet or mobile phone with simple navigation program and combat formation of his group including position of each member and the direction of movement. No one was allowed to retreat, including wounded, punishment – immediate death penalty. Mercenaries from Wagner group also committed war crimes, widely used tortures and unhuman behavior towards Ukrainian military prisoners and civilians. As a result of human wave tactics during the period from December 2022 to April 2023 russian lost near Bakhmut 20 000 – killed in action, 80 000 – wounded, 50% out of them were mercenaries from Wagner group [5, 8, 9].

Lessons learned about of employment of ISR assets during the first year of full-scale invasion are:

disclosure of information did not deter the war, but united the international community, countered russian "false-flag" and information operations;

the United States of America has a significant intelligence capability;

open-source intelligence alongside with commercial assets have played an incredibly important role in revealing russian military buildup on Ukrainian borders, proved russian committed war crimes in Ukraine;

russian concept of operation is not aligned with their employment of tactical ISR assets and SOF.

LIST OF SOURCES

1. President Joe Biden at a press conference on 18-th of February 2022.
https://edition.cnn.com/2022/02/18/politics/joe-biden-russia-ukraine/index.html

2. General Hockenhull, Commander Strategic Command, discussed the use of open-source intelligence at a RUSI Members Webinar. https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war

3. New satellite images show buildup of russian military around Ukraine.
Gianluca Mezzofiore and Tim Lister, CNN.
https://edition.cnn.com/2022/02/02/europe/russia-troops-ukraine-buildup-satellite-images-intl/index.html

4. https://www.youtube.com/watch?v=pzBsWcpmZso

5. Preliminary Lessons from russia's Unconventional Operations During the russo-Ukrainian War, February 2022 – February 2023. Royal United Services Institute for Defence and Security Studies. Jack Watling, Oleksandr V Danylyuk and Nick Reynolds. p. 30-32.

6. Розвідка показала знімки з супутника ICEYE, який був придбаний за пожертви українців. https://mil.in.ua/uk/news/rozvidka-pokazala-znimky-z-suputnyka-iceye-yakyj-buv-prydbanyj-za-pozhertvy-ukrayintsiv/

7. Ukraine at War. Paving the Road from survival to Victory. Royal United Services Institute for Defence and Security Studies. Jack Watling and Nick Reynolds. 4 july 2022, p. 2-18.

8. Preliminary Lessons in Conventional Warfighting from russia's Invasion of Ukraine: February – July 2022. Royal United Services Institute for Defence and Security Studies. Mykhaylo Zabrodskyi, Jack Watling, Oleksandr V Danylyuk and Nick Reynolds. p. 7-12, 24-65.

9. Meatgrinder: Russian Tactics in the Second Year of its invasion of Ukraine. Royal United Services Institute for Defence and Security Studies. Jack Watling and Nick Reynolds. 19 may 2023, p. 1-9, 18-20, 24-25, 29-31.

Розвідка, спостереження та рекогносцировка
Анотація

Стаття допомагає зрозуміти: функції, вплив та зміни в розвідці з моменту повномасштабного російського вторгнення, починаючи з лютого 2022 року. Наголошується на можливостях розвідувального співтовариства США, якому вдалося добути розвідувальну інформацію не тільки щодо самого факту підготовки держави-терориста РФ до повномасштабного вторгнення, а і визначити ймовірну дату його початку. Розсекречування матеріалів та швидке їх поширення забезпечило необхідною інформацією світове співтовариство щодо можливого російського вторгнення. Факт оприлюднення такої інформації на прес-конференції військово-політичним керівництвом США був безпрецедентним в історії людства – адже, зазвичай, така інформація не розповсюджується з метою збереження у безпеці джерела її надходження. Це підкреслило намагання США стримати державу-агресора – РФ від можливого вторгнення. Крім того, цей факт допоміг об'єднати країни-партнери навколо ідеї надання Україні потрібної допомоги та покарання РФ за початок повномасштабного вторгнення в Україну та брутальне порушення всіх можливих міжнародних законів, норм та договорів.

Наголошується на потребі вивчення та врахування інновацій та змін у розвідці, що відбулися протягом першого року повномасштабної російсько-української війни. Використання комерційних супутників дало змогу закордонним репортерам та засобам масової інформації підтвердити факти звірств, катувань та масових вбивств цивільного населення та дітей, які здійснювали російські військові у Бучі та інших містах та селах на тимчасово окупованих державою-терористом українських територіях. Соціальні мережі та засоби масової інформації також відіграли важливу роль у поширенні цієї інформації по всьому світу та інформуванні світового співтовариства про те, що відбувається та факти масових військових злочинів росіян. Крім того, поширення цієї інформації через ЗМІ та соціальні мережі допомогло світовому співтовариству та міжнародним організаціям протидіяти російським інформаційно-психологічним операціям.

Також наведена тактика та приклади штурмових дій приватної військової компанії "Вагнер" та дій росіян на тактичному рівні.

Ключові слова: розвідка, розсекречування інформації, розповсюдження інформації, операція під чужим прапором, розвідка з відкритих джерел інформації (OSINT).