Institute for National Security Studies

Open-Source Intelligence and the War in Ukraine
Author(s): TZ and Tamir Hayman
Institute for National Security Studies (2023)
Stable URL: https://www.jstor.org/stable/resrep47006
Accessed: 03-05-2023 16:38 +00:00

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at https://about.jstor.org/terms

Institute for National Security Studies is collaborating with JSTOR to digitize, preserve and extend access to this content.

This content downloaded from 85.216.55.172 on Wed, 03 May 2023 16:38:54 +00:00
All use subject to https://about.jstor.org/terms

Open-Source Intelligence and the War in Ukraine

TZ and Tamir Hayman | No. 1678 | January 5, 2023

The current war in Ukraine is followed closely by many people throughout the world. The fog of war typical of past wars is strikingly absent this time, thanks to the enormous quantity of open-source information from the battlefield streaming over the internet in real time. Although the war is far from over, at this stage it is already possible to see how the use of open-source intelligence (OSINT), based on commercial capabilities, knowledge-sharing communities on social media, and artificial intelligence tools developed in the private sector have improved the ability of the Ukrainian military to gather intelligence to offset the relative advantage of the Russian military. In November 2022, General Sir Jim Hockenhull, Commander of the UK Strategic Command, which is responsible for the UK's military intelligence organizations, force buildup, and planning, addressed this subject at a virtual conference of the Royal United Services Institute (RUSI). Hockenhull committed to a change of approach among British intelligence organizations. This paper presents the main points of his speech and the recommendations that are also relevant for intelligence organizations in Israel.

"The First Digital War"

The war in Ukraine can be seen as "the first digital war" in history. This term does not refer to fighting abilities based on advanced technology, but rather highlights the dynamic arena in the digital space, close to the battlefield and sometimes within it, with the participation of millions of people and commercial organizations connected to the internet.

The mission of intelligence organizations in war is to gather as much information about the enemy and dispel the fog of battle. Today, in the

This content downloaded from 85.216.55.172 on Wed, 03 May 2023 16:38:54 +00:00
All use subject to https://about.jstor.org/terms

open space it is possible to find commercial satellite photos, technical data collected by media companies (location, activity loads), and a range of content collected and published by individuals on social media. Most of the information used by Ukraine in advance of and during the Russian military invasion was found in the open-source intelligence (OSINT) space. Since the information was largely unclassified, it was possible to analyze it with the help of advanced processing capabilities based on artificial intelligence and developed by the technology giants in the private sector. Data processed in the United States and Britain was easily shared with intelligence organizations worldwide, and particularly in Ukraine, without the policy barriers so familiar to intelligence agents from their routine work. The collected information provided a high-quality response to questions about the Russian invasion such as when and where, and what was the expected scope.

In the digital war, the winner will be the side that is quicker to understand how to exploit the potential of this open space.

The Battle for Hearts and Minds

One of the essential conditions for the ability of the Ukrainian army to repel the Russian forces is the enlistment of international aid. The ongoing support of countries, particularly in the intelligence context but also on military and economic levels, comes from a precise and unprecedented worldwide understanding of the situation on the ground.

Awareness of events in Ukraine was challenged more than once by Russian data warfare and deception. For example, on February 16, 2022, Russia declared its intention to withdraw its forces, but within a few minutes this information was refuted by knowledge-sharing communities on social media. Pictures and live reports flowed in from the field, proving that the forces had not retreated but had actually improved their positions in readiness for the latest invasion plan. This information was critical for the Ukrainian army, but also served the purposes of public diplomacy and the effort to harness public opinion.

This content downloaded from 85.216.55.172 on Wed, 03 May 2023 16:38:54 +00:00
All use subject to https://about.jstor.org/terms

Information warfare and deception are familiar elements of combat doctrines, in the Russian army in particular. Today, intelligence organizations have the growing responsibility to systematically tackle and thwart efforts to introduce fake information. One of the essential capabilities in digital war is "superiority" on social media and platforms for disseminating information, which is measured by the ability to understand the prevailing mood, to issue real time reports rapidly, and to refute rumors with credible sources. In Ukraine, there has been extensive use of civilian action to publicize the course of the fighting and the results of battles – sometimes for the needs of opposing propaganda moves. Clearly the use of open media by the Ukrainian army and civilians led to a more precise grasp of the reality, and a failure of Moscow's war for hearts and minds.

Infinite Number of Sensors and Crowdsourcing

In recent years, the world's militaries, including the IDF, have improved their sensory abilities and increased the number of sensors and means of intelligence gathering about the enemy using advanced military technology. The Ukraine experience demonstrates that every person and every means of communication can be used as a sensor.

According to data from Ukrainian communications companies, the use of public networks helped increase the army's range of reception and broadcast over of its own communications infrastructures. Public networks are deployed with redundancy for the purpose of backup and must routinely pass tests of user and traffic load. In general, these infrastructures are more efficient and more accessible, particularly if the enemy destroys military communications systems. The Ukrainian army adopted the use of civilian infrastructures in the early stages of fighting and thus gained an advantage on the ground.

This represents a significant change in the approach to intelligence gathering, and it is impossible to ignore the ethical and moral challenges of this approach, as the information can invade the privacy of users. However, in times of crisis, such as when the Ukrainian government and people are fighting shoulder to shoulder for survival, the entire public has rallied round

This content downloaded from 85.216.55.172 on Wed, 03 May 2023 16:38:54 +00:00
All use subject to https://about.jstor.org/terms

to lend the homeland an advantage. It is likely that in Israel too, as in the past, the public will support the IDF war effort when necessary.

Furthermore, the public rallied to help the efforts of information gathering in a "crowdsourcing" format. The Ukrainian army utilized discussion platforms where the public was invited to report the activities of Russian forces, their locations, and deployment. A civilian tracking network was set up, which not only doubled observation capacity but also made it possible to vary and expand viewpoints. The army guided the civilians according to its needs and was able to fill in gaps in its information. As the conflict continued, the range of reports submitted by civilians in the field increased.

The Rules of the Game are Changing

Intelligence agents learn that assessing intelligence is like doing a jigsaw puzzle: the picture of the finished puzzle is incomplete, and many pieces are missing. The art of an intelligence agent lies in the ability to position the existing pieces correctly and imagine what the other pieces look like in order to envision the entire picture, based on thorough knowledge of the enemy, research methodology, and information gathering abilities.

Open-source information changes the rules of the game, because it provides many of the missing pieces, particularly in extreme situations such as war. In the war in Ukraine, open-source information filled huge gaps in understanding about the battles and gave more reliable and precise answers than any other source to questions about the extent of damage. This is an important example because these are the issues that occupied the Ukrainian government and decision makers worldwide in debates about courses of actions and the extent of aid.

At the same time, the use of open-source information for intelligence assessment and decision making also has risks. In the example of the jigsaw puzzle, more pieces than required might frame the picture incorrectly in a different, misleading mode – far different from what was presumed. Sometimes that is an excellent way of developing creative thinking and expanding the limits of the imagination, but in times of war, intelligence

This content downloaded from 85.216.55.172 on Wed, 03 May 2023 16:38:54 +00:00
All use subject to https://about.jstor.org/terms

personnel seek means to focus, in order to avoid confusion and bias. In a world where every second 127 new devices connect to the internet and begin spreading content, there is clearly more information than what is needed and more room for interpretations that might steer decision makers in the wrong direction. Therefore, open-source information cannot be sufficient on its own, but only serve as a supplementary layer for classified sources of greater accuracy and reliability.

The important change evident in this context is that whereas in the past military intelligence organizations tended to permit themselves to limit the collection of information in the open sphere and based their assessments and recommendations mainly on classified information, today such a decision would be irresponsible. It would mean dismissing the richness of available and valuable information, and more important, ignoring a central arena of activity in war.

Conclusion

The potential embodied by open-source intelligence is familiar to intelligence organizations in Israel. Dramatic progress in the field has led to global breakthroughs in the ability to collect information, processing based on artificial intelligence and data fusion, and collaborations with industry. Nonetheless, the primary force buildup continues to lean toward classified sources, while the link between the world of classified intelligence and the world of open-source intelligence, and the involvement of civilians and civilian infrastructure in the assessment of intelligence and increased sources of information, is still deemed taboo.

It is still too early to conclude definitively the lessons of the war in Ukraine, but the relationship between the state, military, and intelligence agencies on the one hand, and social media, commercial platforms, and the public on the other, is certainly a wake-up call. Compared to the events in Ukraine it is doubtful whether Western countries, and Israel in particular, are ready to make use of the public and private companies with the same efficiency. However, if we are unable to adopt the new approach now, we will likely not be prepared to tackle the challenges that await us.

This content downloaded from 85.216.55.172 on Wed, 03 May 2023 16:38:54 +00:00
All use subject to https://about.jstor.org/terms

Editors of the series: Anat Kurtz, Eldad Shavit and Judith Rosen

This content downloaded from 85.216.55.172 on Wed, 03 May 2023 16:38:54 +00:00
All use subject to https://about.jstor.org/terms