GOV.UK

Speech

How open-source intelligence has shaped the Russia-Ukraine war

General Hockenhull, Commander Strategic Command, discussed the use of open source intelligence at a RUSI Members Webinar.

From:
Ministry of Defence (/government/organisations/ministry-of-defence), Strategic Command (/government/organisations/strategic-command), and General Sir Jim Hockenhull KBE ADC Gen (/government/people/jim-hockenhull)

Published
9 December 2022

Delivered on: **7 November 2022 (Speaker's notes, may differ from delivered version)**

We shouldn't believe that everything that goes on is always new. Indeed, if we go back to the Foreign Broadcast Information Service from 1941, or the Interdepartmental Committee for the Acquisition of Foreign Publications, we should recognise that this is in a long tradition of exploiting available information. Now this has been scaled at both volume and at pace by the availability of technology, and also the ability of mass to engage in this activity.

There's a lot of confirmation and availability bias in some of the things that we've learned from Ukraine. Because of this we should caveat those lessons slightly and make sure we're applying the right diagnostics and analysis to make sure that we're pulling through the correct lessons.

This is open source for intelligence, but it's also open source and broader understanding which is supporting our intelligence making and decision making. If we can fully understand the availability of this information the impact will go beyond just thinking about intelligence or open source.

Open source fits into a wider set of changes around how we're using information intelligence. The way in which information and intelligence can be declassified, the way in which it has been shared with the public, builds upon a range of changes that are happening in the intelligence space. Much of that is being driven by what's happening in open source, but open source is not the only change. The conflict in Ukraine can in some ways be viewed as the first digital war, and much of that digital

capability is coming from commercially available services rather than necessarily traditional military capabilities.

The availability of commercial satellites has enabled an extension of reach in the Ukrainian military's situational awareness and their ability to conduct surveillance and reconnaissance. We're seeing artificial intelligence used alongside commercial software applications to increase the speed of action. It's also increasing utility. We're seeing an attempt to sense and understand the environment, to decide and orchestrate, to act and then to learn and adapt. Those four stages are about being able to do that with sufficient pace to be able to outpace the adversary, and whoever learns fastest is going to win.

Open source and its role in intelligence has had a significant range of impacts and I would group these into six categories. The first is adding to anticipatory intelligence. How we're understanding the posture of forces and the fusion of commercial imagery, tech data and social media analysis, provided significant insight into Russian deployments. This goes all the way back to spring 2021 through the autumn and winter of 21 into 22, showing us what was happening and where it was happening. That anticipatory intelligence is being used not just by sources inside the military but it's being projected for all to see and for all to interpret.

The second change would be that the impact of conflict is shifting public confidence. We had the ability to share information around Russian activity widely, whether it was in deployment, when fully deployed and postured for invasion, or indeed at point of invasion and beyond. That widely shared a picture has changed the way the public understand how the conflict has taken place. That's true, certainly in Ukraine for example, but it's also true in the wider West. One of the crucial elements of success in Ukrainian conflict has been the commitment of Western nations to provide support. Even if you remember going back to around the 17th of February of this year, Russia started that its forces were redeploying away from the borders. Quickly this was exposed by the open source community which was able to show that not only were troops still in place, but in fact what was happening was a redeployment of force in order to be able to better execute the invasion plan. The public confidence has helped in the utility of being able to share lower classification information with partners.

The third area is countering Russia's Information Operations and countering Putin's own narrative around the war. The pre-conflict deployment and highlighting intent has been important, but also open source has been incredibly important in being able to rebut false flag narratives from the Russians, and indeed, at times has provided the ability to even prebuttal. The fact that the truth was well known meant that as soon as false narratives were put out by the Russians, they were immediately exposed or understood by the public to be a false narrative. That power of information and knowledge has had a really significant impact on the public and been a counter to Russian Information Operations and the false flag operations that were part of the invasion plan. These have failed to be successful, partly, and indeed perhaps largely, as a consequence of the way in which that narrative is able to be exposed as a sham.

Open source has also proved to be a force multiplier, and we've been able to move to an approach which militaries around the world have sought to do for some time. Through open source every platform and every service person is able to act as a sensor. Citizen involvement has meant that practically every citizen and every phone has become a sensor. There are some challenges around the ethical and moral position of this, but in the context of a war of national survival the Ukrainian public are incredibly committed to playing their part and providing the advantage to their decision makers. The second part about the force multiplier is its use of commercial networks. These commercial networks are inevitably driven by a need to keep availability high the people using them, and this means they're incredibly robust. This offers alternative pathways for information to travel and sometimes goes beyond military communications which can be subject to jamming or disruption. It's incredibly difficult to overcome these commercial networks and therefore, that force multiplier of sensors, has been a really significant way in which the Ukraine military have been able to generate information advantage.

The fifth element is in the crowdsourcing and the use of standardised chatbots which has allowed these Ukrainian citizens to report Russian units and locations. The civilian sensor network has been a force multiplier but also, it's been able to provide a variety of viewpoints around information. Rather than having to take a single piece of information and estimate its accuracy, the mass of information is able crowdsource enabling analysts to draw together alternative views. This has enabled processing and evaluation of the availability of data to provide additional insight. The longer the conflict has gone on, the more adept the Ukrainians have become at harnessing the quantity of information to pull insights from as many sensors as possible.

Lastly, in terms of impact of the conflict, there's been an element of lifting the fog of war. I'm a career intelligence officer and certainly, for long periods of my career, it felt like I was responsible for making a jigsaw from the available information. I didn't have the lid of the jigsaw box or sufficient pieces to make the complete jigsaw. This meant I was responsible for putting the pieces I had in place, and then trying to imagine what the rest of the picture would look like to produce a prediction from those assumptions. Whilst open source doesn't provide the lid of the jigsaw box, it gives an almost infinite number of jigsaw pieces. The challenge now is that you can make an almost infinite number of pictures as a consequence of the available pieces. It also introduces a challenge in terms of discretion around the information, and we must filter with a view to being able to refine. This is where the combination of open source intelligence and secret sources of intelligence becomes invaluable in being able to see whether we can define greater understanding as a consequence. There has been some great work in terms of battle damage assessment, and we see a variety of authoritative sources available through social media platforms which provide insight and sentiment analysis. These are incredibly important because it offers the ability to understand what's happening and that has been expanded almost exponentially as a consequence. It also offers the ability to track information operations and assess impact, particularly in Russian information operations. The impact of where things are

being picked up, how they're being proselytised across social media platforms, and tracking and understanding their impact has been really important.

But for all of those impacts, there are of course some risks. The scale of data is beyond comprehension. That creates enormous opportunity but also creates a real burden in terms of being able to deal with intelligence. 127 new devices are connected to the internet every second across the globe and there is a challenge over the veracity of the available information. With more information comes more opinions, more variation, and there really isn't very much more truth. We must accept that the Open Source Intelligence community, which has played a spectacular role in the war in Ukraine, doesn't always get it right. There are moments in time where the community will move off after a particular line of inquiry which turns out to be futile. I've had moments where people have questioned me if this is truly happening as a consequence of what's being carried on social media.

There are limitations with both the scale, the speed, and the veracity of information. We must determine how much automation and augmentation is necessary to be able to divine truth. In the context of Ukraine, open source has been really strong on what is happening, where it's happening, and when it is happening. This strength hasn't been uniform, and there are items where it hasn't been successful, but I think on the whole it's aided that understanding of what, where and when. Where it gets into difficulty is when people take that knowledge and want to describe why things are happening and what's will happen next. The assumptions commentators can make aren't always supported by events and this is absolutely a risk. These situations are where we need to make sure that we're applying our secret sources in combination with open source. Defence has traditionally been good on looking at threat. Most often threat is explained as the threat equals the capability plus intent, but I personally don't believe that's sufficient. We face an increasingly complex and cluttered set of challenges, and we must be better at understanding the context and being able to place the threat in context. For me the equation should be threat equals capability plus intent, divided by the context when the context is largely benign, or multiplied by the context when it's more contested. Open source offers us an opportunity to be able to understand context in a deeper, faster, and more responsive manner than we could do in the past. We gain real power, when we can combine that with secret intelligence and what we gain from our global network.

One of the key things I take away from what's been happening in Ukraine is the need to go much faster than we've gone before in how we exploit open sources. This will need for us to shift our risk calculus, we need to focus on the opportunity cost of not moving fast enough, rather than the challenge over making sure we always comply with legislative policy. We need to make sure that we're able to move both at the speed of relevance but at the speed of necessity. The situation is changing faster than often our ability to understand it and anything that steps in the way of our understanding we need to burn back. We need to look at how we apply different financial freedoms to a much more dynamic engagement with industry, commercial, and open source community. We also need to shift our approach to our people and

understand that there'll be different ways of exploiting open source on behalf of government. We need to look at alternative methods rather than always seeking to want an in-house capability. We need to look at a range of different partnerships and a range of different metrics, including being able to use commercial partners in some fundamentally different ways. I do think the Pareto principle applies to open source, perhaps at the moment open source contributes somewhere in the region of 20% of our current processes, but the availability and opportunity means that we've got to invert this metric. We've got to move on from a place where open source is adding colour and flavour and we need to invert the model so we gain our situational and contextual understanding through open source and combine this with our secret intelligence. We've been talking about doing this for a number of years but the system is still geared towards exploiting secret intelligence, and using the insights it provides around why things are happening and what's going to happen next. It's crucial that we're able to merge those together, but we are going to need to change our thinking and we're going to need to shift our approach. We're going to change our relationship with commercial partners. The power inside government is really going to come through in the cross-referencing, layering and cross-cueing.

There are a range of lessons coming out of Ukraine and this is one of those moments in time where we must reflect. If we don't take due cognisance of what's happening in Ukraine, social media, the commercial world, and inside government, then our system will not be ready and prepared for the next challenge that we face. There is an urgency around the need to change, and I'm going to need the support of the Open Source Intelligence community to help me drive that change into defence.

Published 9 December 2022

Explore the topic

Defence and armed forces (/defence-and-armed-forces)