To cite this article: Duffield, Jack. “The ‘Ukraine Model’ for Intelligence Disclosure May Not be the New Normal”. RUSI. 6 December 2023. https://rusi.org/explore-our-research/publications/commentary/ukraine-model-intelligence-disclosure-may-not-be-new-normal.

# The ‘Ukraine Model’ for Intelligence Disclosure May Not be the New Normal

Jack Duffield

*The war in Ukraine heralded a new era of public engagement for Defence Intelligence. However, the Israel–Hamas war has demonstrated that it is not a silver bullet for countering disinformation.*

In the days and weeks following Hamas’s attack on Israel, and as the Israeli counteroffensive began, no daily intelligence updates were made public by Defence Intelligence in the UK’s Ministry of Defence. This sort of disclosure would not have been expected at all a few years ago. But during the build-up to the 2022 invasion of Ukraine, then-Chief of Defence Intelligence Lt Gen (now Gen) James Hockenhull began briefing publicly that Russia was not drawing down its troops as the Kremlin had claimed. Public commentary on ongoing crises from within the UK’s intelligence establishment was unprecedented at the time. It placed the UK in clear defiance of Russian disinformation, and strongly signalled the UK’s resolve to counter Russian narratives surrounding the war.

This tactic likely emerged as a result of Russia’s 2014 annexation of Crimea. During the invasion of Crimea, NATO identified that persistent military deception – in some cases flatly denying the presence of Russian forces which had already been photographed by media outlets – was a central part of its effectiveness. The NATO STRATCOM Centre of Excellence noted at the time that Western states, the media and the wider public faced a great challenge in identifying and disproving the false narratives that the Kremlin had pumped into the information sphere. When only a few years later Russia repeated its efforts to claim territory in Ukraine with the same disinformation and deception as before, the UK’s novel response offered an immediate antidote which limited Russia’s ability to obfuscate its invasion.

Defence Intelligence followed up with a series of tweeted updates, sometimes more than once a day, drawing hundreds of thousands of views in some cases. Their positive effect was widely acknowledged, with RUSI’s Dr Jonathan Eyal describing last April how the updates ‘crowd out’ Russian disinformation. Even in November 2023, more than 50,000 people a day read these updates on Twitter/X alone, and when Gen Hockenhull was promoted, then-Defence Secretary Ben Wallace singled out the public disclosure of Defence Intelligence products as ‘vital work’ in support of Ukraine.

Given the high regard given to this tool in Defence, its absence in the Israel–Hamas war might seem surprising. After all, there are many similarities between these conflicts. In both cases, an aggressor is weaponising the information environment by pumping out false narratives in support of their strategic end goals. Both conflicts are of significance to Western powers, and both are built upon decades of highly charged and bloody political narratives, in contrast to the often sudden crises which occur elsewhere, such as in the Sahel. However, there are five major differences between these conflicts, each of which offers a lesson for the future employment of public intelligence disclosure.

First, there are the differences between the information environments. Hamas has had success in associating its own extreme ideology, centred on waging war to remove non-Muslims from Palestine and destroy the Israeli state, with the broader Palestinian cause. Massive pro-Palestinian protests from Beirut to London have become organic vehicles for Hamas messaging. Meanwhile, the Kremlin still struggles to obfuscate its direct involvement in small European protests. Hamas also differs from Russia's tendency to publish disinformation in English, instead flooding social media with out-of-context, inflammatory and computer-generated content in Arabic which defies censors. The net result of this is a far greater and faster volume of disinformation in the Israel–Hamas war.

Hamas's tactics are also different. Russia's main goal is gaining control of territory in Ukraine, using combined-arms assault and largely conventional and symmetrical tactics. Hamas desires none of this. It instead aims to generate outrage and create international hostility against Israel. This technique requires an information offensive to be the main effort, rather than a supporting function. Dispassionate and nuanced intelligence disclosures are much less likely to cut through such an emotionally charged narrative.

There are diplomatic benefits to keeping intelligence reporting private. In the case of Ukraine, the UK rallied assistance from states with well-established intelligence relationships, both from the Five Eyes and NATO as well as bilateral partnerships in northern Europe. The regional actors involved in the Israel–Hamas war do not necessarily have these same existing relationships, meaning that bilateral intelligence sharing increases in diplomatic value while public disclosure weakens its effect.

The operational reality is perhaps the starkest area of difference between the two conflicts. There is far more uncertainty in the Israel–Hamas war, partly due to the insurgent nature of Hamas and its tendency to use human shields and medical facilities in operational activity. This is acknowledged in the UK's only major intelligence disclosure of the conflict, where the prime minister stated that a highly contentious explosion at Al-Ahli Hospital in Gaza was 'likely caused by a missile – or part of one – that was launched from within Gaza towards Israel'. After the event, both Israel and Hamas almost immediately blamed each other for the explosion, and the disputed incident created fresh diplomatic rifts in the Middle East. That the UK's comment came six days after the event, with no attribution as to who launched the missile and only a 'likely' assessment rating – indicating a 55–75% probability – speaks volumes about how uncertain the intelligence picture is. Such uncertainty is bread and butter to the UK intelligence community, but is unlikely to resonate with the general public.

A final consideration is the intelligence capability of the aggressor. In the case of Ukraine, Russia has access to a powerful and feared intelligence apparatus with global reach. Very little of the information published by the UK government would have affected Russia's own understanding of the war in Ukraine. Hamas, on the other hand, has very little access to intelligence analysis beyond what is shared by Iran and its regional proxies. It is not unthinkable that daily intelligence updates from the UK might have improved Hamas's ability to coordinate.

To summarise, huge volumes of distributed disinformation, a highly emotive narrative as a central goal, fewer pre-existing regional intelligence relationships, greater operational uncertainty and an aggressor with limited intelligence capability all diminish the value of public intelligence disclosure in the Israel–Hamas conflict. In light of this, the decision not to employ the 'Ukraine model' is completely logical.

These factors also indicate where such an approach might best be used in the future. A potential Chinese invasion of Taiwan would share many traits with the Russian invasion of Ukraine, and public disclosure would likely be similarly potent there. However, conflicts such as the ongoing Sudan civil war have several of the above characteristics in common with the Israel–Hamas war. In cases such as Sudan it is better to avoid the Ukraine model, and this type of conflict is increasingly prevalent.

In the right circumstances, public intelligence disclosure modelled on the UK’s Ukraine updates has been demonstrated as a potent tool. However, it is not a silver bullet for countering disinformation. There are many potential tools available to the UK to combat malign information activities, of which this is only one. Though it may be used again in future by the UK and its allies, public intelligence disclosure is best reserved for the narrow range of crises where it will be most potent.

*The views expressed in this Commentary are the author’s, and do not represent those of RUSI or any other institution.*

## References