Routledge
Taylor & Francis Group

Journal of Policing, Intelligence and Counter Terrorism

ISSN: 1833-5330 (Print) 2159-5364 (Online) Journal homepage: www.tandfonline.com/journals/rpic20

Intelligence and operational warning: lessons from Ukraine

Mike Fowler

To cite this article: Mike Fowler (2024) Intelligence and operational warning: lessons from Ukraine, Journal of Policing, Intelligence and Counter Terrorism, 19:4, 501-518, DOI: 10.1080/18335330.2024.2319128

To link to this article: https://doi.org/10.1080/18335330.2024.2319128

JOURNAL OF POLICING, INTELLIGENCE AND COUNTER TERRORISM
2024, VOL. 19, NO. 4, 501–518
https://doi.org/10.1080/18335330.2024.2319128

Routledge
Taylor & Francis Group

Intelligence and operational warning: lessons from Ukraine

Mike Fowler

Department of Military and Strategic Studies, USAF Academy, Air Force Academy, Colorado, USA

ABSTRACT

This paper examines the challenges of operational analysis as displayed in the Russia-Ukraine conflict. Despite the tremendous success of strategic warning, analysts grossly over-estimated conventional Russian military capabilities and under-estimated the Ukrainians' capability and will. Even after observing Russia's operational capabilities and tactics, analysts again over-estimated Russia's ability to secure Eastern Ukraine. This study finds that poor understanding of military campaigns is the result of six contributing factors. One, *risk management* requires tradeoffs based on competing priorities and finite resources inevitably creating blind spots. Two, there can be *insufficient collection* for operational details due to a focus on strategic requirements or tactical intelligence. Three, an insufficient number of analysts required to cover a breadth of topics leaving them susceptible to challenges like mirror-imaging or single source bias, culminates in *poor analysis*. Four, Russian and Western external and internal strategic narratives were filled with *deception*. Fifth, despite 'need to share' policies, *information stovepipes* continue to plague Western intelligence agencies. Finally, a *lack of professional wargaming* can lead to an analysis-centric view that ignores the valuable expertise of operators and logisticians. Each of these factors contributed to analysts' poor understanding of the operational level of war in the Russia-Ukraine conflict.

ARTICLE HISTORY
Received 27 April 2023
Accepted 2 February 2024

KEYWORDS
Intelligence analysis; warning; strategy; operational; wargaming

Introduction

US warning of the Russian invasion of Ukraine in February 2022 was both an intelligence success and failure. Strategic warning was a tremendous, visible success. It is possible that this disruption to the Russian propaganda campaign delayed the invasion by several weeks requiring ground forces to contend with the mud season. The tactical identification and location of units was also a success that facilitated the strategic warning. At the outbreak of the war, US tactical warning of imminent Russian air attacks likely saved Ukrainian air defences and turned the tide for the Battle of Hostomel Airport (Dilanian et al., 2022, april 16).

But the operational analysis was mostly a failure. Intelligence support to the Chairman of the Joint Chiefs of Staff (e.g. the Defense Intelligence Agency [DIA] and the Joint Staff J2) and the Secretary General of NATO led to public pronouncements of a quick Russian victory. The ground estimate was initially correct. But the quality of units and their

CONTACT Mike Fowler michael.fowler@afacademy.af.edu 2534 Fairchild Dr., USAF Academy, CO, 80840, USA

logistics was grossly over-estimated. Plus, after months of ineptitude from Russian units and their logistics, National Security Advisor Jake Sullivan presented a bleak outlook as the Russians shifted their forces from Kyiv to Eastern Ukraine. Overly dramatic press reports talked about a 'blitz' using terrain more favourable to tank warfare (Samuels, 2022). In March of 2023, the Secretary General of NATO incorrectly predicted that the Russians would capture the small city of Bakhmut within days.

Across every domain, the operational analysis was wrong. Analysts predicted Russian advantages in cyber, airpower, precision missiles, amphibious warfare, and special operations direct action forces would be used to tremendous success. All of those predictions were wrong. The inaccurate operational intelligence is not the fault of an individual analyst, agency, or even country. While some analysts might have had great insights, the general consensus was wrong. Public pronouncements by senior US and NATO military leaders, and the 'common knowledge' of the media and think tank experts were inaccurate.[1]

This work does not seek to summarise the war. Great works by Jonsson and Norberg (2022) as well as Gady and Michael Kofman (2023) provide phenomenal analysis of the war's evolution. Instead, this work will focus on lessons from Ukraine to explore the differences between strategic, operational, and tactical warning and identify those challenges that constrain adequate operational warning despite good strategic and tactical warning.

Intelligence and levels of analysis

There are a surprising number of people that argue that the operational level of war does not exist (Buckel, 2021; Doane, 2015, september 24; Eikmeier 2015; Friedman, 2021; Owen, 2012). At the 2022 International Studies Association annual conference, after David Strachan-Morris presented his paper 'Not an Oxymoron: Developing Theory on Military Intelligence', several national intelligence academic-practitioners argued that operational military intelligence requirements are irrelevant; that military operations could survive off strategic intelligence. The implication was that scraps from the strategic table should be sufficient to feed the dogs of war. While this might be theoretically possible, in practice the requirements for intelligence at the tactical, operational, and strategic levels are inter-related and inform each other, but each is distinct**.**

Conceptualising the different types of intelligence can be viewed from the customer's perspective. For all customers, intelligence is 'the mainly secret activities – targeting, collection, analysis, dissemination and action – intended to enhance security and/or maintain power relative to competitors by forewarning of threats and opportunities'. (Gill & Phythian, 2018, p. 19). The purpose of intelligence is to *use information to reduce uncertainty for a decision maker* (Betts, 1978; Fingar, 2011; Warner, 2002; Wheaton & Beerbower, 2006). While it seems straightforward, there is a plethora of decision makers and decisions to make.

For a junior officer at the tactical level, the differences become readily apparent after requesting analytical assistance from higher headquarters. While the response might be professional and courteous, the products provided are often not useful to the tactical unit. The problem is not a lack of caring. The headquarters has an entirely different frame of reference based on the information their commander needs to make decisions. The intelligence is related but at a different level of detail and a different emphasis. Intelligence

must be tailored to the customer's requirements making it difficult for great products at one level of war to be equally useful at the other levels of war. All intelligence analysis tries to answer the who, what, when, where, why, and how. Yet, Table 1 shows how the level of analysis can vary significantly depending upon the customer.

To answer the 'what' research question above, there are a variety of factors intelligence analysts consider. While the factors may be the same at the different levels of war, Table 2 provides examples of how the different levels of analysis will lead to entirely different collection requirements. Though each level may collect on the same topic, each command has a different requirement for the scope or specificity for the information useful for their decision-making.

Strategic warning is primarily concerned with forecasting the probability that an attack will occur and whether that attack might be nuclear, conventional, or unconventional. While strategic warning is critical to enable forces to prepare, it is insufficient by itself to improve the odds of a successful battle. Operational analysis forecasts how that attack might occur – an alignment of intent, capabilities, and feasibility. Tactical intelligence is primarily concerned with near-real time locating, positively identifying, and tracking enemy forces. For example, US intelligence sharing of tactical tracking of Russian forces enabled several successful Ukrainian strikes against Russian commanders.

Over time, tactical tracking can show patterns from training and combat employment enabling the ability to forecast how the enemy will act during future engagements (Mattis & West, 2019, p. 82). To an extent, tactical intelligence forecasts the best way to engage and defeat an adversary unit. While tactical intelligence is essential, militaries that focus most of their effort on it can overlook critical operational cues. For example, during World War II, the German focus on tactical movements left them with poor operational insight (Ratcliff, 2006, pp. 44–48). As early as 1918 and developed through the 1940s, the US recognised the importance of forecasting (Kries, 1996, pp. 15–16, 22, 390). Despite these lessons, after two decades of focusing on the tactical movements of terrorists, the US ability to conduct operational analysis atrophied (Bury & Chertoff, 2020).

Table 1. Example of intelligence requirements across levels of analysis.

	Strategic	Operational	Tactical
Customer	President, NSC	Theatre commander, Joint task force commander	Unit commander, Mission planner
Who Unit of Analysis	State/Country	Domains	Opposing Unit
What Research question	What is the probability of invasion?	What would an invasion look like?	What is the capability of opposing unit(s)?
When Importance of time	Weeks to Days	Days to Hours	Minutes to Seconds (i.e. near-real time)
Where	Country or Maritime Zone	Region or island group	Specific targets include cities, ports, and airfields
Why	National security objective	Aggregate effect of tactical tasks	Tactical task (e.g. capture or destroy a bridge)
How	Conventional Unconventional Nuclear	Relative effort by: - Domain - Region/route	Typical manoeuvres Firing procedures

Table 2. Varying intelligence requirements.

	Strategic	Operational	Tactical
Level of training and combat experience	Overall military	Service specific (e.g. navy)	Unit specific (e.g. ship, squadron, or brigade)
Equipment quality	Changes in: - Investment in research and development - % of military expenditure to GDP - Growth in military budget	Comparative based on the relative quality of service equipment and proportional quantities.	Comparative - Utilisation rates - Maintenance repair - Weapons range - Probability of kill
Leader characteristics	President or Prime Minister	Service commanders	Unit commanders

For operational analysis, scale is often more important than accuracy to provide a rough planning factor. For example, the difference between 40 and 45 MiG-29 fighters is significant for a tactical planner. The operational planner is typically more interested in scale (tens, hundreds, thousands). For strategic warning, detail on the specific types of fighters is of marginal importance. The knowledge that the country has many fighters and bombers is likely sufficient.

Relative quality is also important. Strategic analysts might focus on the newest technology such as the Russian development of the T-14 tank. Operational analysts would be focused on their proportional representation in front-line forces. While the T-14 might be the best tank in the world, most front-line Russian forces are equipped with the 1970s-era T-72. In the case of the T-72, there are dozens of variants. Tactical planners often want to know which specific variant they will face.

Operational intelligence is for military headquarters: joint task force, component commands (i.e. air, land, space, maritime, cyber, special operations), and combatant commands.[2] *Operational intelligence is the activities that forecast threats and opportunities to reduce a decision maker's risk towards achieving military objectives.* Operational intelligence is a different type of forecasting than strategic or tactical forecasting. Operational intelligence informs decision makers about what to do with assigned forces and when to request additional forces. First, what will the enemy do with all those tactical units and platforms? Threat forecasts are a necessary prerequisite to developing an effective and efficient collection plan, targeting plan, and operational scheme of manoeuvre. An accurate forecast highlights things that need to be protected and methods to disrupt the enemy's intended actions. The second is targeting. Targeting is a forecast of the impact of degrading, destroying, or affecting something. It is a forecast of the impact on future capability, intent, and behaviour. For example, a target analyst may recommend destroying a certain bridge, forecasting that it will delay enemy armour units from crossing a key river for 24 hours as they wait for repairs or manoeuvre to towards an alternate route. Or, an analyst might project that destruction of a certain uranium centrifuge factory would delay the development of a nuclear weapon for six months.[3] Third, over time, it is important for operational intelligence to track the accuracy of its forecast through regular assessments. Collection plans are used to confirm, refute, and test operational planning assumptions about both friendly and adversary actions.

Strategic versus operational versus tactical warning

The levels of analysis are apparent in Erik Dahl's seminal work which finds that 'strategic warning is actually not effective in preventing surprise attacks' (Dahl, 2013, p. 159). Knowledge that an attack is likely is of minimal help. Irregular warfare and 'special operations can succeed quite often despite the loss or absence of strategic surprise … they succeed because of the maintenance of tactical surprise' (Arquilla, 1996, pp. xx–xxi). Dahl argues that countering a surprise attack requires 'very precise, tactical-level intelligence' (Dahl, 2013, p. 173). Based on the framework discussed above, tactical warning is necessary to win the battle, but operational warning can be the key to properly position or prepare forces before the battle.

The Japanese attack on Hawaii was an operational warning problem. While the United States had strategic warning at the national level that some type of attack was imminent, a lack of operational warning meant that both Pearl Harbor and the Philippines were insufficiently prepared for a defence. Plus, a lack of tactical warning (e.g. incoming aircraft, mini-submarines) contributed to a lopsided victory for the Japanese in both operations.

Leading up to the Battle of Midway, strategic warning was sufficient to alert the United States that some type of attack was imminent. However, from an operational perspective, much work was needed to narrow down the area of the attack and the type of capabilities that might be involved. For Midway, operational warning was sufficient to manoeuvre forces in place to win the battle. Certainly, tactical intelligence would have been useful to the defenders on Midway. For example, it could have improved their decision making on when to launch the fighters or bombers or to adjust their defences.

Both sides lacked sufficient tactical intelligence to optimise their defences for each attack wave. This led to significant attrition for both sides. The Japanese lacked both operational and tactical warning. Mechanical failures, and perhaps a lackluster collection plan, led to delayed tactical warning of the threat that the Japanese were facing as the battle began. Strategic warning was critical to ensuring US forces were in the right place at the right time. But, operational warning, and some luck, facilitated an overwhelming US victory.

The Russia-Ukraine case

Russia's 2022 invasion of Ukraine provides an interesting example of a failure in operational warning. The strategic intelligence was a tremendous, and very publicly announced, success providing months of warning of Russia's intent to invade. The tactical level intelligence was adequate as it included: the number of units, unit types, types of weapons and equipment, equipment capabilities and ranges, typical unit manoeuvres and doctrine, and expected avenues of approach (i.e. the primary points of invasion) (Banco, Graff, Seligman, Toosi, & Ward, 2023). But it was not outstanding: it failed to capture that maintenance routines were poor, military warehouses were missing inventory, and conscript training was not well-rounded (Shultz & Brimelow, 2022). Moreover, failure to accurately capture unit quality at the tactical level led to perceptions of Russian conventional ground dominance. Combined, these factors led to over-estimation of the quality of Russian forces. Granted, a massive US intelligence sharing effort provided the Ukrainians a tactical advantage that would have been difficult to forecast.

Operational intelligence had limited accuracy as it predicted the ground scheme of manoeuvre the Russians would use to capture their physical objectives. While it accurately captured intent, there was a gross over-estimation of capabilities while feasibility was largely ignored. Nevertheless, the route of ground forces was accurately predicted as this was primarily governed by their starting point, destination, and the terrain between (Banco 2023). The Chairman of the Joint Chiefs of Staff told congress that Russia would win within a few days.

It was assumed that Russia would dominate across the domains: land, sea, air, and cyber (Dalsjo, Jonsson, & Norberg, 2022). Analysts predicted massive airstrikes, cyber-attacks, and amphibious assaults failed to appear on any significant scale. In part, these assessments were based on significant budget increases and upgraded technology, particularly in missiles (Barabanov, 2011; What They Got, 2017). Russia conducted a major rearmament campaign that culminated in the 'near-total transformation of Russia's armed forces' with 'well-practised [*sic*] transport and logistic capability' (Giles, 2016).

Senior US military officials and think tank experts predicted effective artillery and long-range missile strikes (Banco 2023; Giles, 2021; Persson, 2016, p. 190). Ukraine's air defences would be 'quickly overwhelmed' enabling Russian airstrikes on logistics centres and airfields providing Russia both air superiority while limiting Ukrainian manoeuvre options (Kofman & Edmonds, 2022). Senior US government officials and think tank experts predicted a highly effective Russian cyber offensive to take out Ukrainian C2 (Banco 2023; Courtney & Wilson, 2021; Giles, 2021; Healey, 2022; Miller, 2022). This expectation may have been hyped by announcements by US government officials warning of cyber-attacks as well as a history of cyber surprises including a serious attack on a US oil pipeline in 2021 (Healey, 2022; Miller, 2022). The Black Sea Fleet could hit any part of Ukraine and could conduct a brigade-sized 'significant amphibious operation' (Kofman & Edmonds, 2022).

While the Russians struggled in every domain, the Ukrainians surprised the Director of DIA with their effectiveness (Banco 2023). Ukraine used social media and commercial satellites for targeting (Colom-Piella, 2023). After taking some initial hits, Ukrainian air defence was unexpectedly effective while staying on the move to mitigate the effectiveness of Russian missile strikes (Bremer & Grieco, 2022). Ukrainian troops showed high levels of battlefield innovation, adapting Western weapons to work with Soviet platforms (Colom-Piella, 2023). Plus, Ukraine dominated the information war (Goudsouzian, 2022).

Potential failure points

Using Erik Dahl's framework, the Russia-Ukraine case is a mixed bag of success and failure at the key task to 'produce timely, accurate intelligence' (Dahl, 2013, p. 7; Yengoude, 2017, p. 2). Strategic intelligence was both timely and accurate, mitigating the effectiveness of the Russian 'surprise' attack. But intelligence is more than just about preventing surprise; as Dahl argues, there are three categories of intelligence failures: surprise attack (e.g. Pearl Harbor, 911), an unpredicted major event (e.g. the collapse of the Soviet Union, the Arab Spring), and poor understanding (e.g. underestimation of the impact of Arab Spring on Egypt) (Dahl, 2013). Arguably, the Russia-Ukraine case represents poor understanding at the operational level of war. Phenomenal strategic warning is insufficient to provide operational or tactical understanding (Dahl, 2013, p. 173). Instead of searching for a

single 'root cause' of the problem, this section uses a wide variety of theories across many disciplines to identify six key factors that likely contributed to inaccurate estimates of the military campaign (Jones, 1998, p. 47).

Priorities, decision-making, and risk management

Every commander is faced with making decisions based on limited resources (Lowenthal, 2020, p. 70; Nuechterlein, 1976, pp. 256–259). Obtaining the type of intelligence to develop good operational understanding requires rigorous planning and an extensive collection network. However, this is only an option when the issue becomes a high enough priority. This can be problematic as commanders make tradeoffs to balance chronic security risks against emerging problems.

For a commander to re-assign resources to a new mission requires an intelligence signal significant enough to change the operational priorities. The intelligence process is a zero-sum game. Putting resources onto a mission that might happen often takes away from a mission already occurring. The commander accepts the inherent risks associated with the decision to re-assign intelligence resources. Accepting risk is a factor of competing priorities, probabilities, and potential consequences.

From a risk management perspective, there can be a tendency to focus on worst-case scenarios since failure to predict those would have the most severe impact. For example, leading up to the Russian invasion of Ukraine, US and NATO intelligence priorities would likely be interested in Russian national security decisions, nuclear weapons development, the hypersonic missile program, and cyber-attacks on infrastructure. While US European Command would undoubtedly be interested in Russia's conventional force, those analysts would also be responsible for other theatre problems such as finding and tracking terrorists and Russian activity in the Arctic. In some cases, emphasis on tactical intelligence pushes operational understanding to the back burner (Bury & Chertoff, 2020). While a commander controls their assigned assets, some collection such as cyber, space, or open source might be controlled at the national level. When competing for those assets, the requirements might be outprioritised by national requirements or another command. For example, US combat operations in Syria would have a significant, competing demand for operational and tactical intelligence.

Arguably, the US has a track record of over-estimating conventional militaries while under-estimating unconventional forces. Perhaps the wars that the US military plans to fight differ significantly from those it conducts. 1990s Iraq was grossly over-estimated (Woodford, 2016). It had one of the largest armies in the world, stocked with war-hardened veterans and top-of-the-line Russian equipment and French upgrades to their integrated air defence system and modern French fighters. While the Iraqis had over a 900 aircraft, they could only support launching a few dozen at a time. With antiquated surface-to-air missiles and radar coverage focused on Iran and Israel, the Iraqi air defence system was not designed to withstand a massive air campaign (Singh, 2022).

A few years later, NATO forces assumed that defeating the Serbian forces would be easy since they had similar equipment to Iraq (Kay, 2000; Lake, 2009). But militias used unconventional tactics such as urban warfare and effectively used terrain to hide from airpower. By 2002, Iraq's military was a shell of what it was in the 1990s (Cordesman, 2002). Air defences were non-existent. Equipment was antiquated and in poor repair. Reliance on conscripts and a lack of recent conventional war resulted in a 'green' army. Military

leadership was chosen for their loyalty rather than their military or organisational competence; they were perceived as incompetent 'yes-men'. Again, the use of unconventional warfare, the rise of an insurgency, and the importance of tribal politics were not adequately projected (Perry et al., 2015).

In each case, the place and type of war that was waged was not previously on that commander's list of concerns. Throughout the 1980s, Iraq was a US ally. After the collapse of communism, Yugoslavia was not a serious threat. While efforts were being made to construct Afghanistan in 2002, commanders and planners assumed that the second war with Iraq would be a short-term stay. After all, the first war was over quickly and the US firepower advantage was even more lopsided in 2002. While Libya was a priority for preventing international terrorism in the 1980s and 1990s, after 2001 Libya became an ally in the global war on terror. When NATO went to war in 2011, there was limited insight into the inner workings of the Libyan civil war or to the extent that the government was willing to go. If the planning priorities drive intelligence processing, then intelligence gaps are bound to appear. Yet, it goes a little too far to argue that Russian military forces were being ignored. Particularly after the Russian invasion of the Crimea in 2014, think tank research and defence blog articles on the Russian military were somewhat common.

Insufficient collection

When a country is a low priority for intelligence collection, it is logical that there will be poor understanding beyond things that are easy to collect. In the cases above, these countries transitioned from low priority to top priority quickly. The intelligence community had little time to move the necessary assets and personnel. Re-tasked analysts had scant historical evidence to identify trends, informal networks, or to understand key decision-making processes.

In the Russia case, time was not a serious constraint. The invasion came eight years after the Russian invasion of the Crimea and the execution of unconventional operations in Eastern Ukraine. Yet, it is likely that intelligence collection was not focused on the Russia-Ukraine border. In the Spring of 2021, the Ukrainian military warned their American counterparts that the Russians were building up forces on the border. Despite the repeated warnings, US intelligence was not convinced anything was unusual until fall of 2021 (Stewart, 2023). By October, US analysts were forecasting that a Russian invasion was possible.

Russia would certainly have been a high priority intelligence collection before the invasion. Even so, it is likely that the Ukraine-Russian border was not a top priority relative to other security issues in Russia. Based on the planning priorities, the limited number of Russian experts would likely focus on nuclear weapons, cyber, space, national decision-making, internal stability, and emerging technology such as hypersonics. It is possible that they were not well-versed in the slang, idioms, values, and habits of Russian logisticians and supply clerks.

If Russian conventional forces did warrant a high priority, the intelligence collection might not have been designed to support the level of detail required. Commanders and analysts in Iraq and Afghanistan were often inundated by the plethora of collection assets giving some the illusion that they could eliminate the fog of war (McMaster, 2008, p. 26). Of course, the Russian case did not have that level of scrutiny involved. While

certainly some collection assets were assigned to Russia, there is a lack of flexibility in the intelligence bureaucracy. The system creates disincentives to share collection assets between agencies, services, and missions. Therefore, operational analysts must rely on what they can get.

Unfortunately, data that is easy to get and quantify may not be the most informative (Freedman, 2010; Greenhill & Staniland, 2007, p. 384). Imagery is easy to collect, enabling simple quantitative comparisons of tanks, missiles, and aircraft. Using imagery for qualitative analysis of equipment requires a high revisit rate and long-term familiarity with habits and procedures. Unfortunately, some imagery analysts are assigned based on their familiarity with the sensor regardless of their lack of familiarity with the collection target. For example, after two decades of focusing on irregular warfare groups with makeshift equipment, the Russian Army might appear high-class in comparison. Getting the level of detail necessary to identify the flaws in the Russian military machine would need more intrusive intelligence measures such as communication intercepts and human intelligence.

Poor analysis

Analysts are susceptible to a long list of logical fallacies and cognitive errors that can lead to faulty assumptions and inaccurate conclusions (Davitch, 2022; Gill & Phythian, 2016; Heuer, 1999; Howard, 1962; Jervis, 2006). Arguably, confirmation bias is the more prominent error, which creates a 'human tendency to pay attention to the signals that support current expectations' (Wohlstetter, 1962, p. 392). For example, despite numerous clues and indicators during World War II, the Germans gravitated towards those bits of information that supported their belief that the German high-tech communications encryption, Enigma, had not been compromised (Ratcliff, 2006). Overcoming this bias can be particularly difficult when other public announcements, media articles and think tank reports come to similar conclusions. Even when based on the same data, this type of circular reporting can give a piece of evidence more credibility or impact than it might otherwise deserve.

Analysis can also be influenced by mirror imaging – the analyst places their own value set or belief system upon the intelligence target.[4] Mitigating mirror imaging requires an empathy for others gained through in-depth understanding of others' (enemy, neutral, partner) perspectives, interests, processes, values, and cultural beliefs. Culture influences preferences which shape strategic options and planning assumptions (Drohan, 2016, pp. 232–233).

Arguably, the Russians never intended to use airpower in the Western way of war (Pietrucha, 2022). The Russian Air Force lacked precision munitions, targeting pods, and quality flight training (Bronk, 2022). Russian space capability provides limited, infrequent satellite imagery with poor resolution (Luzin, 2022, may 24). Plus, all intelligence is routed through Moscow, taking days to reach tactical warfighters (Bronk, Reynolds, & Watling, 2022; Peck, 2023). Russian airpower is simply not designed for quick-reaction targeting.

Even their ground forces lack flexibility. The Russian military does not have an effective NCO corps, it does not delegate authority, and has a tradition of punishing initiative which makes military forces slow to react and unable to exploit opportunity (Barany, 2023). The lack of room for creativity resulted in many 'frontal assaults on entrenched positions' (Lee & Kofman, 2022).

Of course, gaining that level of understanding presumes that a sufficient number of analysts are assigned to study the problem. But, over time, the US intelligence community has dramatically increased the variety of problems it studies without a corresponding increase in analysts. This amplifies that classic 'signals vs. noise' problem (Wohlstetter, 1962, p. 387).

Lack of time for in-depth understanding can lead some to rely upon a historical analogy (May & Neustadt, 1986; Rittel & Webber, 1973; Speller, 2011). Massive exercises, surprise inspections, and sustained combat operations in Syria showed a resurgent military and demonstrated Russian strategic mobility in their ability to deploy troops (Facon, 2019; Persson, 2016). Meanwhile, Russian expeditionary capabilities in Syria demonstrated power projection combat capabilities. With short rotations of troops, the operation enabled high rates of combat experience with new weapon systems including unmanned aerial vehicles and precision munitions. In retrospect, the capabilities in a small-scale counterinsurgency were not a good reflection of Russia's potential to conduct a massive ground offensive on multiple fronts.

Some analysts are biased towards a single source, failing to leverage the benefits of an approach that integrates all sources (Wirtz & Rosenwasser, 2010). These preferences can lead to dismissing of 'unofficial' analyses published in unclassified venues. Any unclassified product would be missing the insights of the analyst's favourite, sensitive source (Davitch, 2017; Weinbaum, 2021). Arguably, this may have contributed to a lack of insights into the impact of sanctions on Russia. Over time, steel sanctions enacted in 2014 reduced the quality of new equipment and impaired the maintenance of old equipment. New Russian tanks had weak armour without imported steel and relied upon shoddy munitions.

For decades, admonishments that Russia is not '10-feet tall' seemed to have little impact on threat projections (Depetris, 2018; Depetris, 2020; Keller, 1961; Muskie, 1981; Ullman, 2020). At least two academics predicted that the impacts of Russian cyber-attacks would be negligible (Maschmeyer & Kostyuk, 2022). Years of responding to Russian cyber-attacks combined with US training would mitigate the impacts of future attacks. Analysis indicated that ground forces heavily relied on old equipment despite investments and suffered manning problems limiting the number of deployable units (Persson, 2016, pp. 190–193). Three months before the invasion Lt Col Alex Vershinin publicly noted that Russian logistics were going to be a major problem (Vershinin, 2021). He noted that Russian logistics depended heavily on rail, which would work well up to the border. But once over the border, the Ukrainian rail lines were incompatible with Russian trains. What is interesting here is that Vershinin is not an intelligence officer, but an army armour officer with experience in sustainment experiments. Personnel issues were highlighted as a challenge – difficulties with calling up reservists, lack of qualified noncommissioned officers, lack of initiative, and training that focused on set-piece exercises that look good but have little relation to combat capability (Giles, 2017).

Despite the cliché to never attack Russia during the winter, the terrain and weather in the Winter of 2022 attracted little attention. During the Russian invasion of Ukraine, armour forces found that terrain that was perfect for tanks throughout much of the year could periodically become sinking, mud pits. While the senior commanders might have been oblivious, some tactical units were aware: just two weeks before the invasion several Russian tanks near the Ukraine border required heavy ground-moving equipment

to extricate their vehicles from deep mud (Malyasov, 2022). The mud constrained the mobility of Russian manoeuvre forces, making them easier targets for missiles and ambush teams. This also created chokepoints and traffic jams that disrupted movement and resupply.

Deception at multiple levels

This case considers deception against multiple audiences: the Russians against the West, the Russians themselves, and the West against themselves. Labelling this case as an analytical problem presumes that somehow, somewhere there was evidence of Russian fallibility. The Russians have a historical fondness for deception. The Russian narrative promoted a message of strength while down-playing weaknesses (Keller, 1961; Ullman, 2020). Putin presented a two-week projection to capture Kyiv as a mathematical certainty. The Russian narrative about military transformation gave outsiders the impression that they were over-powered relative to Ukraine. Perhaps the leadership convinced themselves that the Russian army could execute a logistically ambitious plan with 'too many objectives from too many axes of advance' (Lee, 2022).

It is also possible that the Russian leadership was unaware of their weaknesses due to both active and passive internal deception. With active internal deception, certain actors within the Russian military actively deceived the military and political leadership. Defence industrialists, quartermasters and maintenance chiefs deceived their superiors to hide their corruption (Crowther, 2022). In this context, Russian decision makers lacked critical data to inform their analysis.

Internal passive deception is created in cultures that promote 'yes-men'. Organisational behaviour that punishes negative news and rewards positive news leads to a system that over-emphasises its capabilities while hiding weaknesses from military and political leaders. For example, in Saddam Hussein's 1990s Iraq, senior advisors preferred to misinform Saddam rather than risk his ire by giving him bad news. In this case, decision makers have both over-estimates of their own capabilities and under-estimates of their adversary.

This type of misinformation campaign could be pervasive throughout Russian military culture. Sloppy techniques and inadequate resources for preventative maintenance including poor training, high turnover ('not my conscript problem … let the next guy deal with this'), lack of funding, and a lack of NCO cadre create a combination of policies, procedures, funding priorities, and behaviours that led to units being unaware of their own vulnerabilities during peacetime. Based on these internal dynamics, Putin could easily have been convinced that the relatively small special operation was filled with high quality, highly skilled troops that would be greeted by the locals as liberators.

These issues are evident in the sinking of the Russian Black Sea Flagship, Moskva. With significant anti-air capabilities, the Moskva was sunk by the firing of two anti-ship missiles. Despite impressive capabilities on paper, a lack of training would render the crew unable to defend the ship and incompetent at real-life damage control. 'If Russia's Army is any indication of how well they have been maintaining and upgrading their equipment, I feel sorry for their Navy' (personal communication with Commander Andrew Gerla, US Navy, 19 April 2022).

Of course, the Russians are not the only ones that deceive themselves. In the weeks leading up to the war, Ukrainians commanders did not take the Russian threat seriously

which gave their US counterparts the impression that their units were unprepared for a conflict (Stewart, 2023).

Even without the US and NATO, bureaucratic politics can play a role as competition for resources occurs between services and commanders who may perceive that their domain (air, land, sea) is the most critical to the operation. This can encourage, consciously or not, an exaggeration of the threat to improve the justification for more resources (Aspin, 1981, p. 168). Like the journalism cliché, 'if it bleeds, it leads', commanders that are focused on resource fights will have a large appetite for new, high-tech developments (Peitrucha, 2015). This is not to suggest that commanders are lying to get more money. But the fear of technologically falling behind the adversary can effectively motivate action. Examples include the bomber gap, the missile gap, the space race, and more recently, the race to build hypersonic missiles. Convinced of their own strong beliefs, commanders may 'ignore subordinates or assemble their own teams of analysts to confirm their biases' (Walcott, 2023).

Information stovepipes

It is also possible that some analysts had great insights, but institutional stovepipes prevented information sharing. Institutional stovepipes can prevent analysts from sharing key pieces of the puzzle with each other or even from sharing their overall assessment. For example, suppose that a Russian land analyst had the perfect assessment but that the national analysts supporting the Pentagon were unaware of the assessment or did not bother to consult the expert.

After the 2012 attack on the Benghazi consulate, Ambassador Susan Rice's intelligence talking points erringly referred to the attack as a protest that turned spontaneously violent. Some analysts had known for several days that the attack was pre-planned by individuals linked to terrorist groups (Hudson, 2022). In the first hour of the attack when data was limited, reports of lots of people surrounding the consulate seemed similar to violent protests at US embassies in Egypt and Yemen. But, once the MQ-1 Predator arrived on-scene, providing data-linked full-motion video, it became quickly apparent that the event was not a protest. While political opponents claimed this was a poorly designed cover-up, more likely is that the analyst(s) supporting Rice's interviews simply did not know about the video. There are always analysts who may think they have sufficient information to make an assessment without taking the time to consult an expert that might live in a different time zone.

Despite transitioning from 'need to know' to 'need to share' policy, each intelligence organisation has virtual analytic boundaries. Intelligence organisations, like all bureaucracies, create incentive structures to focus on their own mission and prioritise meeting the needs of their own customers (Wilensky, 2015; Zegart, 2007a, 2007b). Intelligence is not intentionally hidden from other organisations. But few bureaucracies have incentive structures that encourage sharing with outsiders. Due to concerns over competition and the potential lack of reciprocity, 'most organisations are more concerned with how best to control information than how best to share it' (McChrystal, 2015, p. 141, 174).

There are analytic divisions within each organisation based upon variations in sub-organisational intelligence problems, domains, and priorities. Ideally, the divisions enable specialisation emphasising unity of effort. Unfortunately, these divisions

sometimes contribute to inter-service, inter-agency, and regional analytic rivalries. Rivalry creates several intelligence sharing challenges: disincentives to share, incompatible communication systems, unique security compartments, and different lexicons.

For example, there were special operations teams training Ukrainian forces in Ukraine for several years before the invasion. Presumably, the trainers had good insights into the capabilities and motivation of Ukrainian soldiers. Likely, they also knew that mud season had an impact throughout large areas of Ukraine that would make manoeuvring problematic. Certainly, some Ukrainians knew. While these trainers could provide great insights to the intelligence community, the system is not designed that way. There is no method for intelligence analysts to send a requirement to operations. While trainers might do an after action report, there is no requirement to share it with the broader intelligence community. Special operations teams are secretive in nature and unlikely to share their report with anyone not required.

Lack of wargaming

Wargaming is an important part of the US and NATO planning process to test plans for adequacy and feasibility. For it to be adequate, the plan would use a quantity and quality of a suitable capabilities to achieve the objectives. The Russians brought all the right equipment in large amounts. A wargame would have highlighted that the majority of Russian equipment was antiquated. An analysis of feasibility captures the realm of what is possible (physically, virtually, and cognitively). Ground-centric wargames place a premium on the effects of terrain and weather which would have signalled the manoeuvre problems faced by the Russians.

Plus, a wargame would have forced a more detailed analysis of Ukrainian forces. While the Ukrainian Navy had limited capability, analysts did not seem to account for the threat of Ukrainian anti-ship missiles to the Russian Black Sea Fleet. Analysts assumed that Ukraine's conventional forces were essentially doomed and that their best option would be to create an insurgency with hit-and-run tactics (Hammes, 2021; Kofman & Edmonds, 2022). A well-designed cyber wargame would have shown that Russian cyber would be marginal. After 2014, Ukraine invested and trained in cyber defence. Most cyber-attacks are 1-hit wonders making it easier for Ukraine to defend itself as Russia continued to reuse its limited stockpile of cyber weapons (Greenberg, 2017). A wargame would provide a more balanced view of potential outcomes.

Unfortunately, wargaming at the operational level is often skipped or done poorly due to the time and expertise required to develop the game. The experts needed to help design the game are the same ones that are needed to analyse the adversary or to create and execute the operations. Plus, military wargaming is typically only done for two purposes: to test the effects of a new military technology; or to test a US/NATO operational plan. It is not typically used to assess how someone else's war is going to play out. But, in some cases, it should be.

Wargames are not a panacea. They can be used superficially like any analytical tool. There are a variety of bad wargames: using a single play to find 'the answer', mis-designing the game to create a predetermined answer, or ignoring a critical but complex domain such as cyber or information operations. Plus, they will not necessarily help focus on the correct scenario. Planners did wargames for the invasion of Iraq, but the games focused on the capture of Baghdad, not the occupation (Benson, 2020).

An effective wargame requires experts on strategic approaches, operational capabilities, and other key stakeholders such as partner countries. To mitigate classification bias, the games should include an integration of both academics, intelligence professionals, and military planners. To maximise the utility of the game results, detailed analysis will need to be conducted to determine logistical limitations and feasibility of operations. If necessary, multiple iterations of the game can be played with varying levels of maintenance and logistics success to provide a broad range of best-case and most likely-case scenarios.

Conclusion

The evidence suggests that no single factor contributes to poor understanding at the operational level of war. A combination of historical cases and the Russia-Ukraine case suggest that poor understanding of campaigns or the operational level of war are the result of a combination of six key contributing factors. First, risk management and opportunity costs result in intelligence assets and personnel resources focused on missions that are extremely important. Fortunately for the world but unfortunately for intelligence warning, it is those less important missions that result in combat operations. Second, when assets are dedicated to the mission, they are focused on strategic and tactical requirements leaving significant gaps in operational understanding. Third, mirror-imaging, confirmation bias, and poor use of historical analogies continue to plague analysis. Fourth, the ability to see through adversary deception is problematised both by their own internal self-deception and by a Western sensitivity to technological developments. In other words, many dictators believe their own hype, and many analysts, government employees, and journalists buy into it. Fifth, bureaucratic politics and organisational behaviour create information stovepipes. Despite heroic efforts to increase intelligence sharing, finding a current assessment on an evolving crisis is not always easy. For outsiders, it is not obvious where the information is or even which classification network should be searched. Insiders might be hesitant to share it with outsiders without submitting it to lengthy and thorough review process, particularly if going to senior decision-makers. Finally, detailed wargaming at the operational level is necessary to facilitate identification of intelligence gaps and improve estimates outcomes of military missions.

Operational warning does not guarantee victory. It must work in concert with strategic and tactical warning. Planners need warning across all three levels of war to devise an effective strategic, operational, and tactical plan. And, that plan needs to be well-executed by competent operators. While the US had made great improvements in its strategic and tactical warning, the Russia-Ukraine case suggests that there is significant room for improvement in the US and NATO ability to provide operational warning. This study identified six potential contributing factors: risk management, insufficient collection, poor analysis, deception, information stovepipes, and lack of wargaming. It would be nice to pick one of those factors as the root cause. Yet this study finds no evidence to discount any of the factors. Instead, each had some impact. A detailed, internal analysis of the US Intelligence Community and NATO military analysis would be useful to refine options for improving operational analysis for the next major conflict.

Notes

1. Over time, declassified sources might show that some analysis was correct but not made public.
2. With a direct line to the Secretary of Defense and subordinate joint task force commanders, US combatant commands frequently need both strategic and operational intelligence.
3. The US Air Force considers the targeting of war-related industry a 'strategic attack' – these tactical missions are intended to have strategic effects. This muddling of the levels of war convinces some that strategic intelligence should focus on war-related industry. See Kries, 1996, p. 2.
4. The psychology term for this is 'projection'.

Disclosure statement

No potential conflict of interest was reported by the author(s). This is the work of the author and does not necessarily reflect the opinion of the US Air Force Academy. PA#: USAFA-DF-2023-357.

References

Arquilla, J. (1996). *From Troy to Entebbe: Special operations in ancient and modern times*. Lanham, MD: University Press of America.

Aspin, L. (Summer 1981). Misreading intelligence. *Foreign Policy*, *43*.

Banco, E., Graff, G.M, Seligman, L., Toosi, N, & Ward, A. (2023, February 24). 'Something was badly wrong': When Washington realized Russia was actually invading Ukraine. *Politico*.

Barabanov, M.2011). *Russia's new army*. Moscow: CAST.. http://amzn.to/2fCxbc2.

Barany, Z. (2023). Armies and autocrats: Why Putin's military failed. *Journal of Democracy*, *34*(1), 80–94. doi:10.1353/jod.2023.0005.

Benson, K. (2020). *Fighting the CENTCOM OIF campaign plan: Lessons for the future Battlefield*. Modern War Institute.

Betts, R. K. (1978). Analysis, war, and decision: Why intelligence failures are inevitable. *World Politics*, *31*(*1*), 61–89. doi:10.2307/2009967.

Bremer, M. K., & Grieco, K. A. (2022). In denial about denial: why Ukraine's air success should worry the West. *War on the Rocks*.

Bronk, J. (2022). The mysterious case of the missing Russian Air Force. *RUSI*.

Bronk, J., Reynolds, N., & Watling, J. (2022). The Russian air war and Ukrainian requirements for air defence. *RUSI*.

Buckel, C. (2021). A new look at operational art: How we view war dictates how we fight it. *Joint Force Quarterly*, *100*(94–100).

Bury, P., & Chertoff, M. (2020). New intelligence strategies for a new decade. *RUSI Journal*, *165*(4), 42–53.

Colom-Piella, G. (2023). The bear in the labyrinth. *RUSI Journal*, *167*(6-7), 72–81. doi:10.1080/03071847.2023.2177193

Cordesman, A. H. (2002). *Iraq's military capabilities in 2002: A dynamic net assessment*. Center for Strategic and International Studies.

Courtney, W., & Wilson, P. A. (2021, December 8). If Russia invaded Ukraine. *RANDBLOG*.

Crowther, A. (2022). *Russia's Military: Failure on an Awesome Scale*. Center for European Policy Analysis.

Dahl, E. (2013). *Intelligence and surprise attack*. Georgetown University Press.

Dalsjo, R., Jonsson, M., & Norberg, J. (2022). A brutal examination: Russian military capability in light of the Ukraine War. *Survival*, *64*(3), 7–28. doi:10.1080/00396338.2022.2078044

Davitch, J. M. (2017). Open sources for the information age: Or how I learned to stop worrying and love unclassified data. *Joint Force Quarterly*, *87*, 18–25.

Davitch, J. M. (2022). *Do not trust your gut: How to improve strategists' decision making*. Strategy Bridge.
Depetris, D. (2018). Despite the bluster, Russia Is Not 10 Feet Tall. *The National Interest*.
Depetris, D. (2020). The big hack is damaging. That doesn't make Russia 10 feet tall. *Defense One*.
Dilanian, K., Kube, C., Lee, C.E., & De Luce, D. (2022, April 16). U.S. Intel helped Ukraine protect air defenses, shoot down Russian plane carrying hundreds of troops. *NBC News*. Retrieved from https://www.nbcnews.com/politics/national-security/us-intel-helped-ukraine-protect-air-defenses-shoot-russian-plane-carry-rcna26015.
Doane, L. M. (2015, September 24). It's just tactics: Why the operational level of war is unhelpful fiction and impedes the operational Art. *Small Wars Journal*.
Drohan, T. A. (2016). *A new strategy for complex warfare*. Amherst, NY: Cambria Press.
Eikmeier, D. C. (2015). Operational Art and the Operational Level of War, are they Synonymous? Well It Depends. *Small Wars Journal*.
Facon, I. (2019). Military exercises: The Russian Way. In S. J. Blank (Ed.), *The Russian military in contemporary perspective* (pp. 219–248). Carlisle, PA: Strategic Studies Institute.
Fingar, T. (2011). *Reducing uncertainty: Intelligence analysis and national security*. Stanford, CA: Stanford University Press.
Freedman, D. H. (2010). Why scientific studies are so often wrong: The streetlight effect. *Discover*.
Friedman, B. A. (2021). *On operations: Operational Art and military disciplines*. Annapolis, MD: Naval Institute Press.
Gady, F. S., & Kofman, M. (2023). Ukraine's strategy of attrition. *Survival*, *65*(2), 7–22.
Giles, K. (2016). *Russia's 'New' tools for confronting the West: Continuity and innovation in Moscow's exercise of power*. London: Chatham House: The Royal Institute of International Affairs.
Giles, K. (2017). *Assessing Russia's reorganized and rearmed military*. Carnegie Endowment for International Peace.
Giles, K. (2021). *Putin does not need to invade Ukraine to get his way*. Chatham House.
Gill, P., & Phythian, M. (2016). What is intelligence studies? *The International Journal of Intelligence, Security, and Public Affairs*, *18*(1), 5–19. doi:10.1080/23800992.2016.1150679
Gill, P., & Phythian, M. (2018). *Intelligence in an insecure world*. Medford, MA: Polity Press.
Goudsouzian, T. (2022). How Ukraine won the information war. *The National Interest*.
Greenberg, A. (2017 June 20). *How an entire nation became Russia's test lab for cyberwar*. Wired.
Greenhill, K. M., & Staniland, P.. (2007). Ten Ways to Lose at Counterinsurgency. *Civil Wars*, *9*(4), 402–419.
Hammes, T. X. (2021). *Guerrilla tactics offer Ukraine's best deterrent against Putin's invasion force*. Atlantic Council.
Healey, J. (2022). *Preparing for inevitable cyber surprise*. War on the Rocks.
Heuer, R. J. (1999). *Psychology of intelligence analysis*. Center for the Study of Intelligence.DC: Central Intelligence Agency.
Howard, M. (1962). The use and abuse of military history. *RUSI Journal*, *107*, 4–10.
Hudson, J. (2022). Susan rice blames bad Benghazi Intelligence for her misleading version of events. *The Atlantic*.
Jervis, R. (2006). Understanding beliefs. *Political Psychology*, *27*, 641–663. doi:10.1111/j.1467-9221.2006.00527.x
Jones, M. D. (1998). *The thinker's toolkit: 14 powerful techniques for problem solving*. New York: Three Rivers Press.
Jonsson, M., & Norberg, J. (2022). Russia's war against Ukraine: Military scenarios and outcomes. *Survival*, *64*(6), 91–122. doi:10.1080/00396338.2022.2150429
Kay, S. (2000). After Kosovo: NATO's credibility dilemma. *Security Dialogue*, *31*(1), 71–84. doi:10.1177/0967010600031001006
Keller, W. (1961). *Are the Russians ten feet tall?* London: Thames and Hudson.
Kofman, M., & Edmonds, J. (2022, February 22). *Russia's shock and awe: Moscow's use of overwhelming force against Ukraine*. Foreign Affairs.
Kries, J. F.1996). *Piercing the fog of War: Intelligence and Army Air Forces Operations in World War II*. Air Force History and Museums Program.

Lake, D. R. (2009). The limits of coercive airpower: NATO's 'victory' in Kosovo revisited. *International Security*, *34*(1), 83–112. doi:10.1162/isec.2009.34.1.83
Lee, R. (2022, April 30). Rob Lee on why attrition will be a critical factor in the battle for Donbas. *The Economist*.
Lee, R., & Kofman, M. (2022, December 23). *How the Battle for the Donbas Shaped Ukraine's Success*. Foreign Policy Research Institute.
Lowenthal, M. M. (2020). *Intelligence: From secrets to policy* (8th Ed.). Thousand Oaks, CA: CQ Press.
Luzin, P. (2022, May 24). Russia's space satellite problems and the War in Ukraine. *Eurasia Daily Monitor*, *19*.
Malyasov, D. (2022, February 11). Over a dozen Russian tanks stuck in the mud during military exercise. *Defence Blog*.
Maschmeyer, L. & Nadiya Kostyuk, N. (2022, February 8). There is no cyber 'shock and awe': plausible threats in the Ukrainian conflict. *War on the Rocks*.
Mattis, J., & West, B. (2019). *Call Sign Chaos: Learning to lead*. New York: Random House.
May, E., & Neustadt, R. (1986). *Thinking in time: The uses of history for decision makers*. New York: The Free Press.
McChrystal, S. (2015). *Team of teams: New rules of engagement for a complex world*. New York: Penguin`.
McMaster, H. R. (2008). On War: Lessons to be learned. *Survival*, *50*(1), 19–30. doi:10.1080/00396330801899439.
Miller, M. (2022, January 28). Russian invasion of Ukraine could redefine cyber warfare. *Politico*.
Muskie, E. S. (1981, February 1). Soviets aren't 10 feet tall. *The Washington Post*.
Nuechterlein, D. E. (1976). National Interests and Foreign Policy: A conceptual framework for analysis and decision-making. *British Journal of International Studies*, *2* (3), 256–259. doi:10.1017/S0260210500116729
Owen, W. F. (2012). The operational level of war does not exist. *The Journal of Military Operations*, *1* (1), 17–20.
Peck, M. (2023, March 29). Why Russian space satellites are failing in the Ukraine War. *Popular Mechanics*.
Peitrucha, M. W. (2015). Capability-based planning and the death of military strategy. *Proceedings*.
Perry, W. L., Darilek, R.E., Rohn, L.L., & Sollinger, J.M. (2015). *Operation Iraqi freedom: Decisive war, elusive peace*. Santa Monica, CA: RAND.
Persson, G. (2016). *Russian military capability in a ten-year perspective – 2016*. Swedish Defence Research Agency.
Pietrucha, M. (2022, August 11). Amateur hour part II: Failing the air campaign. *War on the Rocks*.
Ratcliff, R. A. (2006). *Delusions of intelligence: Enigma, ultra, and the end of secure ciphers*. Cambridge: Cambridge University Press.
Rittel, H., & Webber, M. (1973). Dilemmas in a general theory of planning. *Policy Sciences*, *4*(2), 155–159. doi:10.1007/BF01405730
Samuels, B. (2022, April 4). White House warns of potential Russian blitz on eastern Ukraine. *The Hill*.
Shultz, R.H. & Brimelow, B. (2022). *Russia Potemkin army*. Modern War Institute.
Singh, M. (2022, October 19). Looking back at Iraqi air defences during operation desert storm. *From Balloons to Drones*.
Speller, I. (2011, February 24). *The use and abuse of history by the military*, Paper presented at Desmond Tutu Centre for War and Peace Studies at Liverpool Hope University. Retrieved from http://eprints.maynoothuniversity.ie/3843/1/IS_Use_Abuse_History.pdf.
Stewart, B. (2023, March 24). *Comments from the Senior Defense Official to Ukraine, 2021-2022*. Presentation at National Character and Leadership Symposium. US Air Force Academy, CO.
Ullman, H. (2020, February 12). *Politics of fear: China and Russia aren't 10 feet tall*. UPI.
Vershinin, A. (2021). Feeding the bear: A closer look at Russian army logistics and the fait accompli. *War on the Rocks*.
Walcott, J. (2023). Why the press failed on Iraq. *Foreign Affairs*.
Warner, M. (2002). Wanted: A definition of intelligence. *Studies in Intelligence*, *46*(3).

Weinbaum, C. (2021, April 12). The Intelligence Community's Deadly Bias Toward Classified Sources. *RAND Blog*.

What They Got. (2017, January 8). *Russian defense policy*. Retrieved from https://russiandefpolicy.blog/2017/01/08/what-they-got.

Wheaton, K. J., & Beerbower, M. T. (2006). Toward a new definition of intelligence. *Stanford Law & Policy Review*, *17*, 319–330.

Wilensky, H. (2015). *Organizational intelligence: Knowledge and policy in government and industry*. New Orleans, LA: Quid Pro Quo Books.

Wirtz, J. J., & Rosenwasser, J. J. (2010). From combined arms to combined intelligence: Philosophy, doctrine, and operations. *Intelligence and National Security*, *25*(6), 725–743.

Wohlstetter, R. (1962). *Pearl Harbor: Warning and decision*. Stanford: Stanford University Press.

Woodford, S. (2016, May 17). *Assessing the 1990-1991 Gulf war forecasts*. The Dupuy Institute.

Yengoude, E. A. (2017). The enemy achieves surprise: Are intelligence failures avoidable? *Journal of Political Sciences and Public Affairs*, *5*(4), 1–5.

Zegart, A. B. (2007a). 9/11 and the FBI: The organizational roots of failure. *Intelligence and National Security*, *22*(2), 165–184. doi:10.1080/02684520701415123

Zegart, A. B. (2007b). Cnn with secrets:' 9/11, the CIA, and the organizational roots of failure. *International Journal of Intelligence and Counterintelligence*, *20*(1), 18–49. doi:10.1080/08850600600888581