ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Transforming the Intelligence Cycle through Adapting to Complex Environments and the Operational Dynamics of Special Warfare

Emir Muhić | Department of Security Studies, Faculty of Criminalistics, Criminology and Security Studies, Bosnia and Herzegovina | ORCID: 0009-0007-3752-4341

Abstract

In today's increasingly complex and dynamic international environment, intelligence services are confronted with the phenomenon often referred to as special warfare, understood here as the combination of kinetic and non-kinetic threats such as information manipulation, cyberattacks, political subversion, and the involvement of organised criminal groups. While similar multi-domain challenges have existed in earlier periods, including during the Cold War and the global war on terror – the speed, technological dimension, and volume of contemporary operations create qualitatively new pressures on intelligence structures. This paper, using a conceptual and comparative methodological approach, critically reviews the existing scholarship on the intelligence cycle and examines case-inspired dynamics of special warfare to assess whether a network-based model can more effectively reflect these demands. The analysis consolidates critiques of the traditional linear cycle, develops a model emphasising simultaneity, adaptability, and real-time cooperation between analysts, operators, and decision-makers, and identifies institutional and cultural challenges of implementation. The study does not claim that such challenges are entirely unique to the present, but argues that digitalisation

Received: 25.06.2025

Accepted: 07.10.2025

Published: 07.11.2025

Cite this article as:
E. Muhić, "Transforming the intelligence cycle through adapting to complex environments and the operational dynamics of special warfare," ACIG, vol. 4, no. 1, 2025, doi: 10.60097/ACIG/211788.

Corresponding author:
Emir Muhić, Department of Security Studies, Faculty of Criminalistics, Criminology and Security Studies, Bosnia and Herzegovina; E-mail: emirmuhic@fkn.unsa.ba
0009-0007-3752-4341

and cyber-based domains accentuate the limitations of linear approaches. It concludes that the networked approach, while not replacing the traditional cycle completely, represents an important adaptation in intelligence work with implications for both national security practice and the theoretical advancement of intelligence studies.

Keywords

network model, adaptive approach, complex environment, intelligence cycle, special warfare

Introduction

The contemporary international environment is often described as marked by instability, overlapping crises, and interaction across military, political, economic, informational, and social domains. Although such multidimensional challenges are not entirely unprecedented – intelligence services in earlier periods, including the Cold War and the fight against transnational terrorism, also operated under conditions of uncertainty. The current landscape differs in the unprecedented speed of information flows, the scope of digital interconnectedness, and the proliferation of cyber-based methods. Decision-makers increasingly rely on intelligence assessments to navigate this environment, yet the traditional intelligence cycle, developed in the mid-20th century and grounded in linear, bureaucratic logic has been criticised for its limited ability to keep pace with these evolving threats. In such a setting, intelligence structures are not only required to process larger amounts of data at greater speed but also to deal with actors and methods that deliberately blur the boundaries between war and peace, state and non-state activity, and kinetic and non-kinetic operations. These dynamics are frequently analysed through the concept of special warfare.

The notion of special warfare has been defined differently across military and intelligence traditions. In the ex-Yugoslav doctrinal context, it was described as a set of coordinated political, economic, psychological-propaganda, intelligence-subversive, and military activities carried out to gain influence and intervene in the internal affairs of another state, where the use of armed forces remained secondary to other means of influence [1, 2]. By contrast, North Atlantic Treaty Organization (NATO) and the US doctrine usually use the term special warfare in the narrower sense of special operations, understood as actions of highly trained forces

using unconventional techniques to achieve tactical or operational results, while broader non-kinetic threats are categorised under the label of hybrid warfare [31]. The Russian perspective is again different: Moscow formally uses the concept of a 'special military operation', which is positioned below the threshold of full-scale war and seeks to achieve political-military goals through a single decisive operation rather than prolonged strategic campaigns [4].

In this paper, the term special warfare is employed in the broader, multi-domain sense derived from the Yugoslav tradition, which highlights the combined use of political, informational, subversive, and limited military means to achieve strategic objectives. This choice is deliberate: it distinguishes the argument from the Western preference for hybrid warfare and from the Russian usage of special operation. It also allows for a direct conceptual link between special warfare and the intelligence cycle, since both deal with the interaction of diverse instruments of power under complex and dynamic conditions. Since special warfare relies on simultaneity, deception, and multi-domain pressure, it exposes the rigidity and slowness of the traditional intelligence cycle more directly than conventional conflict. Recent conflicts, such as the war in Ukraine, illustrate how cyber operations, propaganda, and conventional military actions interact simultaneously, forcing intelligence structures to adapt in real time.

The paper first outlines the traditional intelligence cycle and its limitations, then situates these in the context of modern complex environments and special warfare. It proceeds to propose a network-based adaptive model, discusses its operational applicability, and illustrates its use through several hypothetical examples before concluding with key findings.

2. The Traditional Intelligence Cycle and Its Limitations

The origins of the intelligence cycle can be traced back to the late 1940s, when LTC Phillip Davidson and LTC Robert Glass introduced a schematic model of tactical military intelligence in their manual *Intelligence is for commanders* (1948), prepared for the US Army Command and General Staff College. The model was designed primarily for military commanders as a tool for planning, collection, processing, analysis, and dissemination of intelligence in support of battlefield operations. Although originally intended for tactical use, the cycle quickly became institutionalised and adopted more broadly within intelligence communities. This bureaucratic

framing reinforced the perception of the intelligence cycle as a linear process that could reduce uncertainty through order and structured steps. The intelligence cycle is an important tool for every analyst and intelligence officer. It is a thought process used to create an intelligence product that responds to the needs of the end user or another actor, and at its core, it's a structured transformation of raw data and information into knowledge that supports decision-making. According to the US Director of National Intelligence (DNI) [5], the intelligence cycle is the process through which information is collected, converted into intelligence, and delivered to policymakers and consumers. Essentially, it includes receiving guidance from the client; collecting information in response to that guidance; analysing the information to evaluate its reliability and usefulness; and producing assessments or predictions based on the client's questions [6]. This process is often adjusted by different actors depending on their needs. For example, the US Federal Bureau of Investigation (FBI) defines six phases in the intelligence cycle: requirements, planning and direction, collection, processing and exploitation, analysis and production, and dissemination [7]. On the other hand, the Central Intelligence Agency (CIA) follows five phases: planning and direction, collection, processing, analysis and production, and dissemination [8]. Such structured phases are effective in areas like organised crime investigations, counterintelligence, or counterterrorism, where targets and indicators evolve more slowly and data sets can be standardised. However, critics note that in complex and fast-changing environments, such sequential steps often appear insufficient. For instance, during the Russian campaign against Ukraine, cyber intrusions, disinformation, and covert paramilitary actions occurred simultaneously, which made it difficult to apply a strictly sequential collection–analysis–dissemination logic. This is especially true when dealing with threats coming from special warfare operations and offensive actions conducted by state actors. Of course, earlier periods, such as the Cold War or the 'war on terror', also confronted intelligence services with simultaneity and multi-domain threats; what appears different today is the speed of cyber operations, the digital saturation of the information space, and the volume of real-time data to be processed.

The borderless nature of many of today's threats has created a space of uncertainty, an idiom of unease, and a need to rethink the collection and analysis of intelligence far beyond state-to-state matters [9]. These actors often use a multi-domain approach and adapt to the environment they are operating in. Additionally, threats often occur simultaneously and in parallel, and require a multi-phase approach within the intelligence cycle. Like almost every other

part of the modern state bureaucracy intelligence has increasingly developed into a 'networked' effort, involving not only state agencies but also public–private partnerships and hybrid actors [9, p. 24]. Criticism of the traditional intelligence cycle is largely directed at its excessive linearity and oversimplified representation of complex processes. It has been noted that it is 'an inadequate description of what actually happens in intelligence work. It is too linear, too rigid, and fails to account for the complexity of modern intelligence processes' [10, p. 959]. Hulnick also emphasises that 'it is not a particularly good model, since the cyclical pattern does not describe what really happens', adding that 'the intelligence cycle also fails to consider either counter-intelligence or covert action', both of which are essential components of contemporary operations [10]. Another problem lies in the assumption that intelligence work follows an orderly and sequential process. In reality, as Hulnick explains, collection and analysis often occur simultaneously rather than in separate stages, and 'if the intelligence cycle really worked as designed, the circulation of raw reports to policy officials would not happen' [10, p. 962]. This discrepancy between theory and practice highlights the limits of the traditional model in reflecting how intelligence is actually produced and used. A critical stance towards the intelligence cycle is also articulated by Evans [11, p. 22], who observes that 'the character of warfare in the 21st century has become notably more complex, concurrently emphasising these traits while introducing new pressures on the intelligence function and application of the Intelligence Cycle'. Drawing on Hulnick's critique [10], Evans [11] further notes that the traditional model is 'fundamentally flawed, as its component parts do not accurately describe the activities of the intelligence mechanism in either the order – or form – they take place', and that it 'does not accurately reflect the practice of counter-intelligence, as the latter is driven by its own separate principles which do not meld with those underpinning the Intelligence Cycle' [11]. While acknowledging these limitations, Evans [11] also cautions that counter-intelligence operates in a mutually reinforcing relationship with the intelligence cycle, rather than outside it, since it relies on and feeds information produced through the process. Doctrinal debate has similarly stressed that it is 'precisely when people tried to use the cycle as procedural clockwork that the weaknesses of thinking of it as a mechanistic cycle were mostly like to be exposed' [12, p. 11]. In other words, the traditional model shows significant limitations in contemporary operational environments, as it is overly linear and too slow for situations that require rapid decision-making and greater agility. Its mechanistic logic may still function in long-term problems where time is not a critical factor, but in dynamic and unpredictable

contexts, the cycle risks becoming an obstacle rather than a support to the decision-making process [12].

Faced with such simultaneity and complexity, scholars and practitioners have sought alternative models that break away from the rigid sequential order of the classic cycle. Arguably, this attempt at broad societal involvement has become the catchword and cornerstone of Western security policies – a rhetoric of resilience and robustness which Europe labels 'the comprehensive approach' and the US has deemed 'the all-of-nation approach' [9, p. 22]. One attempt to respond to these challenges is the concept of the *target-centric intelligence process*, proposed by Clark [13]. In this model, the focus is on the target itself. According to Clark [13], the aim is to build a shared understanding of the target, from which all participants can extract relevant information for their tasks, and to which everyone can contribute with their resources or expertise to create the most accurate picture. In other words, the intelligence cycle and its processes are organised around the target, and all activities are adjusted to fulfill the intelligence requirement based on that central goal. Because traditional cycles may not fully capture the speed and dynamic nature of operations within special warfare, which are often shaped by strategic goals but executed through rapidly changing tactics, scholars have suggested the need to explore new frameworks. This creates the rationale for exploring a network-based model of the intelligence cycle, one that emphasises simultaneity, adaptability, and multidirectional communication, as discussed in the next section.

3. The Modern Complex Environment and the Dynamics of Special Warfare

Today's international environment, where various state actors operate, is highly competitive and often hostile. It is shaped by asymmetric threats, high levels of uncertainty, and an increasing overlap of military, political, economic, and informational domains. With no clear global hegemon or bipolar world order, countries like China, Russia, and alliances like the European Union (EU) have taken on global roles, alongside the still dominant United States. In addition to major powers, regional actors, such as Turkey, Israel, Iran, and North Korea, are gaining influence. Many of them either possess or are close to acquiring nuclear capabilities, which elevates their importance on the global stage. Alongside states, non-state actors also play a significant role. Theorists, such as Kilcullen, describe these threats as either 'dragons', state actors like Iran, North Korea, Russia or 'snakes', non-state actors such as criminal

organisations, drug cartels, and terrorist groups [14, pp.18, 36]. This diversification of threats blurs the traditional line between internal and external security and demands an interdisciplinary intelligence response.

The nature of modern threats has led to a departure from the state-centric security model focused on conventional military threats. Although propaganda, subversion, and terrorism are not new phenomena, their combination with digital interconnectedness and cyber capabilities has multiplied their reach and speed. Today, security is challenged by non-kinetic actions like propaganda, indoctrination, political subversion, and cyber-attacks on critical infrastructure that target the political and social systems of a state. Modern security, therefore, is no longer about physical dominance alone but also about managing perceptions, narratives, and social norms. These non-kinetic threats aim to influence beliefs, values, and cultural attitudes in society through psychological manipulation, rather than physical destruction. At the same time, kinetic actions, such as terrorist attacks, assassinations, and physical cyberattacks, are also being carried out.

These combined operations aim to overwhelm a state's capacity to detect, analyse, and respond effectively. This is known as the saturation effect, where a state's resources become overstretched. A well-documented example is the 2008 Russia–Georgia conflict, where cyberattacks on government servers were launched simultaneously with military incursions and disinformation campaigns, leaving Georgian authorities unable to coordinate a coherent response. Other examples, such as Russian operations in Crimea in 2014 or ongoing cyber campaigns against Western states, similarly demonstrate how multi-domain tactics interact. Hybrid environment defines special warfare as a multi-domain and multi-phase form of conflict, and it uses a mix of covert force and strategic information manipulation to erode institutional legitimacy and social cohesion. The diversity of threats and methods makes it increasingly difficult for national intelligence services to maintain effective security, though the exact scale of this increase is hard to measure empirically. Countries such as the United States, Russia, and Israel commonly use these unconventional tactics. Their approach may differ depending on political goals, capacity, and available resources, but the core objective remains the same: to shape the perceptions of specific groups. Special warfare often includes propaganda, indoctrination, blackmail, and political pressure, which serve to justify or prepare the ground for kinetic actions carried out by military or paramilitary actors. For example, Russian

operations in Crimea in 2014 combined local proxy militias, political manipulation, and massive disinformation campaigns to create confusion and justify subsequent military intervention. This creates a tactical-operational illusion that confuses targets and makes it difficult to distinguish real threats from deception. Due to the complex nature of these operations, intelligence analysts must adopt a broader and more flexible approach to provide useful insight for decision-makers. Critics argue that the traditional intelligence cycle, while still useful as a didactic model, lacks the responsiveness and adaptability required in real-time decision-making environments. This gap opens the door for network-based models of intelligence, where simultaneity and constant feedback replace rigid sequential steps.

4. Limitations of the Classical Intelligence Cycle in a Complex Environment

The classical intelligence cycle, long regarded as a core tool of analysis and decision support, has been increasingly criticised as inadequate when applied to environments dominated by special warfare and complex, fast-evolving threats. Its formal structure, derived from rational bureaucratic models of the 20th century, assumes clear phases, predictable information flows, and linear causality. In practice, contemporary intelligence challenges are non-linear, multidirectional, and deliberately shaped by adversaries who exploit ambiguity, deception, and information saturation. As Lowenthal [15] notes in *Intelligence: From secrets to policy*, the intelligence process must be understood as a holistic system of stages, requirements, collection, analysis, and dissemination, rather than a linear progression, suggesting the necessity of more integrative, network-based models. This tension suggests why the cycle, although still embedded in doctrine, often struggles to reflect the realities of modern operations. In recent years, many in the intelligence community have concluded that the intelligence cycle is no longer valid as the exclusive organisational principle [16]. Additionally, in the American intelligence discourse, there are now voices calling for the intelligence cycle to be killed [16].

Various versions of the intelligence cycle illustrate its institutional rigidity. For instance, Goldman [7] describes it as a sequence of requirements, planning and direction, collection, processing and exploitation, analysis and production, and dissemination. The CIA [8] presents a slightly streamlined variant that omits exploitation, while Korać [17] conceptualises it as a process of planning and organising, followed by collection, processing, analysis and

production, and finally sharing and feedback. Despite these differences, all versions preserve a linear structure that assumes predictable information flows and sequential causality.

Although these models differ slightly, they all share a linear and sequential logic that assumes intelligence is produced in discrete stages and delivered as a finished product. To resolve that paradox, the 'collection' part of the intelligence cycle is at times almost writ out of the practice of intelligence as such, reduced to a neutral activity necessary for, but also somehow preceding and external to, the 'real thing'; the act of information 'processing' [9, p. 26]. Critics argue that such an approach risks becoming too rigid for the speed and complexity of special warfare, where operations combine kinetic and non-kinetic measures, such as cyberattacks, information operations, and deception campaigns, that unfold in real time. As Warner [18] notes, decision-making today occurs at computer speed, placing pressure on traditional phase-based processes.

Importantly, the intelligence cycle is primarily a Western/NATO construct, embedded in military doctrine (e.g. FM-2-0 [17], MCWP 2-10 [42]). By contrast, countries, such as Russia and China, rely on more centralised and integrated intelligence models, where the boundary between collection, analysis, and operations is blurred. Chinese 'three warfares' (legal, psychological, and media) and Russian 'active measures' demonstrate how intelligence is directly tied to influence and political action, rather than treated as a separate analytical process [19–21]. This integration can reduce institutional inertia and accelerate decision-making, although it may also reflect political structures, rather than an inherent functional superiority.

The weakness of the traditional cycle also lies in its inability to define where the process begins. Morris [22] observes that clients cannot request intelligence on unknown targets, underscoring that intelligence is often generated through exploratory collection rather than linear tasking. Clark [13] therefore proposes a model where clients participate actively throughout, creating a dynamic and adaptive loop instead of a unidirectional process. Evans [11] further stresses that crises demand immediate results, exposing how the traditional cycle is too slow to meet operational needs. Beyond speed, critics highlight deeper epistemological concerns. Krohley warns against the overreliance on technology, quantitative metrics, and the illusion of total situational awareness [23]. Such tendencies risk undermining critical thinking and contextual interpretation, skills essential when adversaries deliberately manipulate or falsify data. To counter this, analysts must reintroduce reflection,

uncertainty, and interpretation into their work. Similarly, Gill and Phythian [24] identify challenges such as bureaucratic politics, technological disruption, and interactive complexity, all of which call for network-based multi-flow intelligence processes, rather than a rigid cycle. Recent operational experience confirms these critiques.

Recent operational lessons in Ukraine lend support these critiques. Dinerman [25] demonstrates how the introduction of fusion cells in Iraq and Afghanistan reduced isolation between special operations forces and conventional units, enabling integrated targeting, situational awareness, and faster decision-making. Fusion cells represent *ad hoc* or semi-permanent structures, where collection, analysis, and operational functions are integrated within a single team, enabling real-time information-sharing and rapid decision-making across institutional boundaries. Russia's 2008 war in Georgia and the 2014 annexation of Crimea further underline the point: success depended less on linear intelligence products and more on real-time integration of surveillance, psychological operations, and political action. The ongoing war in Ukraine provides another example, where both Russian and Ukrainian forces increasingly rely on rapid sensor-to-shooter loops, open-source intelligence, and decentralised decision-making to adapt continuously in real time. In the US counterinsurgency campaigns in Iraq and Afghanistan, commanders frequently bypassed the formal cycle to rely on fusion cells that combined collection, analysis, and operations in the same structure. As Dinerman [25] notes, fusion cells reduced operational isolation between Special Operations Forces (SOF) and conventional units, enabling integrated targeting and faster decision-making. These examples illustrate that modern intelligence is not produced in a step-by-step chain but emerges dynamically from the interaction of multiple domains and actors. While the classical intelligence cycle continues to serve as a useful pedagogical model and a baseline framework, many scholars argue that it no longer provides a sufficient guide for the realities of special warfare and complex operational environments. Its linear structure makes it difficult to capture deception, ambiguity, and simultaneity. For this reason, scholars, such as Evans [11], Clark [13], Warner [18], Morris [22], Krohle [23], and Gill and Phythian [24], advocate for adaptive, networked, and interactive models. These approaches aim to capture the fluidity of intelligence production and align more closely with the multi-domain, high-tempo character of contemporary operations. A growing body of scholarship has already critiqued the limitations of the 'traditional' intelligence cycle [10, 24, 12] often pointing to its linearity and bureaucratic rigidity. This paper builds on those critiques but seeks to move

beyond them by operationalising a network-based alternative that not only emphasises multidirectional flows and real-time feedback but also provides practical mechanisms, such as interoperable digital platforms, fusion centres, and adaptive training frameworks that translate conceptual debates into institutional reforms. In this way, the contribution lies less in identifying the weaknesses of the classical model, and more in outlining a pathway for embedding adaptability into daily intelligence practice.

5. Transforming the Intelligence Cycle: From a Linear Model to Adaptive Networks

The modern security environment is frequently described as characterised by unpredictable threats, rapid technological advancement, and strong interaction between military, political, economic, informational, and social domains. In such a setting, traditional intelligence models, often seen as overly bureaucratic, have been criticised as insufficient and in need of redefinition. Because of these challenges, scholars and practitioners increasingly explore adaptive, flexible, and multi-layered approaches. These models do not follow a strict sequence of steps, but instead allow different phases to occur simultaneously and influence each other. Special warfare, cyber threats, and information manipulation are just some of the modern phenomena that require intelligence work to be continuously adaptable. Analysts now need to skip steps, move backward, work in parallel, and include decision-makers directly in the process of analysis and interpretation. Recent critiques emphasise that without such flexibility, intelligence risks becoming irrelevant in fast-moving environments dominated by deception and disinformation. The traditional intelligence cycle, based on four to six clearly defined hierarchical phases, is increasingly seen as less useful in environments where massive volumes of information move at high speed and threats develop across many interconnected fronts. Instead of fixed and separate steps, modern intelligence processes often include additional phases and sub-phases, giving analysts more flexibility and allowing a better fit with specific operational needs. Operational experiences since the early 2000s illustrate why intelligence processes have evolved towards more adaptive formats, with additional phases and sub-phases added in practice. This is particularly visible in the ongoing war in Ukraine, where intelligence work has relied less on step-by-step processes and more on rapid integration of operational, informational, and psychological actions in real time. For example, the *planning and direction phase* now includes tasks such as risk source assessment, mapping actors in the information space, and proactively identifying influence operations.

Rather than just receiving requests, planning involves constant dialogue with decision-makers and adjusting goals in real time. The *collection phase* goes beyond traditional HUMINT, SIGINT, and IMINT methods. It now includes sub-phases like real-time social media monitoring and collection (SOCMINT), cyber reconnaissance, disinformation tracking, and automated data collection through algorithms and artificial intelligence (AI). These new methods require specialised skills and technologies. The *analysis and production phase* has expanded to include predictive analytics, scenario modelling, social network analysis, and big data processing. Analysis is no longer just human reflection; it also involves automated tools and behaviour prediction models. Even the *dissemination phase* is changing. Instead of sharing final products through formal channels, today's distribution often happens in real time using mobile-friendly formats, interactive maps, and dynamic platforms that allow users to search and analyse data based on their own needs. As Clark [13] emphasises, this represents 'intelligence as a living process', where clients are not passive recipients but active collaborators.

These new sub-phases are not fixed or universal. They depend on factors like: (a) the type of threat (e.g. special warfare with non-kinetic threats vs. conventional threats), (b) the domain of operations (e.g. cyber, social media, and economy), (c) the technological environment, (d) available resources, and (e) strategic goals of intelligence operation. This shift is often described as a fundamental change in how intelligence agencies organise their work. However, it is more accurate to view it as a gradual institutional adaptation, where modular, scalable, and mission-tailored systems supplement, rather than fully replace linear models.

Conventional cycle models imagine clear phases arranged in a line or circle. Yet, in today's world of special warfare, fast-changing technologies, and multi-domain conflicts, intelligence services are increasingly turning towards network-based models.[1] Another development that has challenged the validity of the intelligence cycle is the creation of a networked log shared by all parties, which in wartime allows all participants to provide and receive updates in real time [16]. In these models, phases are no longer strictly sequential or separate. Instead, they act as nodes in a network, connected by multiple communication channels. Planning, collection, analysis, and dissemination happen in parallel, iteratively, and flexibly. Information moves not only 'forward', but also 'laterally', 'backward', and 'across'. As Johnston [26] shows in his ethnographic study of analytic culture within the US intelligence community, intelligence analysis is influenced by multiple cognitive, organisational,

[1] As some of the models, the following can be mentioned: network-centric model, target-centric intelligence cycle, collaborative intelligence analysis, complex adaptive system, and so on.

and contextual variables that interact in complex ways. This recognition underlines the inadequacy of rigid sequential approaches and provides strong support for network-based intelligence models that better reflect the realities of analytic practice. This multidirectional flow mirrors what Krohley [23] and Gill and Phythian [24] describe as the move from cycles to networks, where intelligence is produced through continuous interaction rather than linear progression. This makes it possible to make quick course corrections and keep intelligence updated in real time. As shown in Fig. 1, the network model replaces linearity with multidirectional connections between phases, while Fig. 2 provides a simplified example of how such redesign works in practice.

This networked approach brings several important advantages:

- Flexibility where teams can work simultaneously on different tasks, and cognitive processes don't require a fixed order, which speeds things up.
- Speed – decisions can be made in real time, which is essential in special warfare, where reaction time can determine success or failure.
- Resilience, where system supports itself through redundancy and collaboration.
- Better adaptation to information warfare and complex threats through fluid and dynamic nature of the information environment requires constant updates and analysis, not waiting for one phase to finish before starting the next.

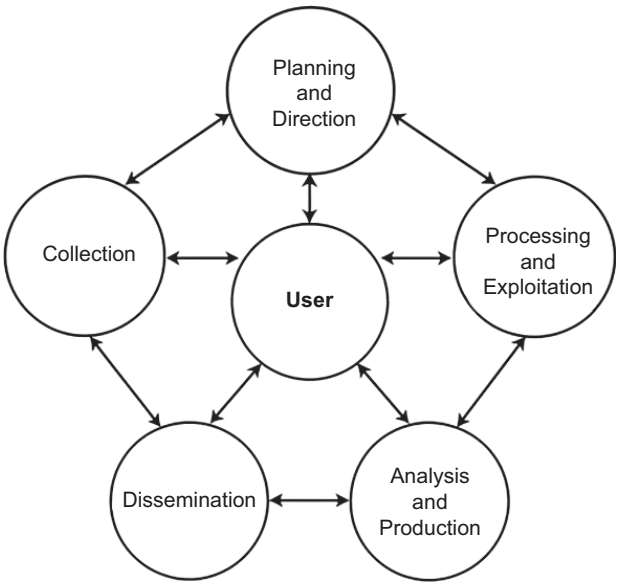

Figure 1. Network model of the intelligence cycle.

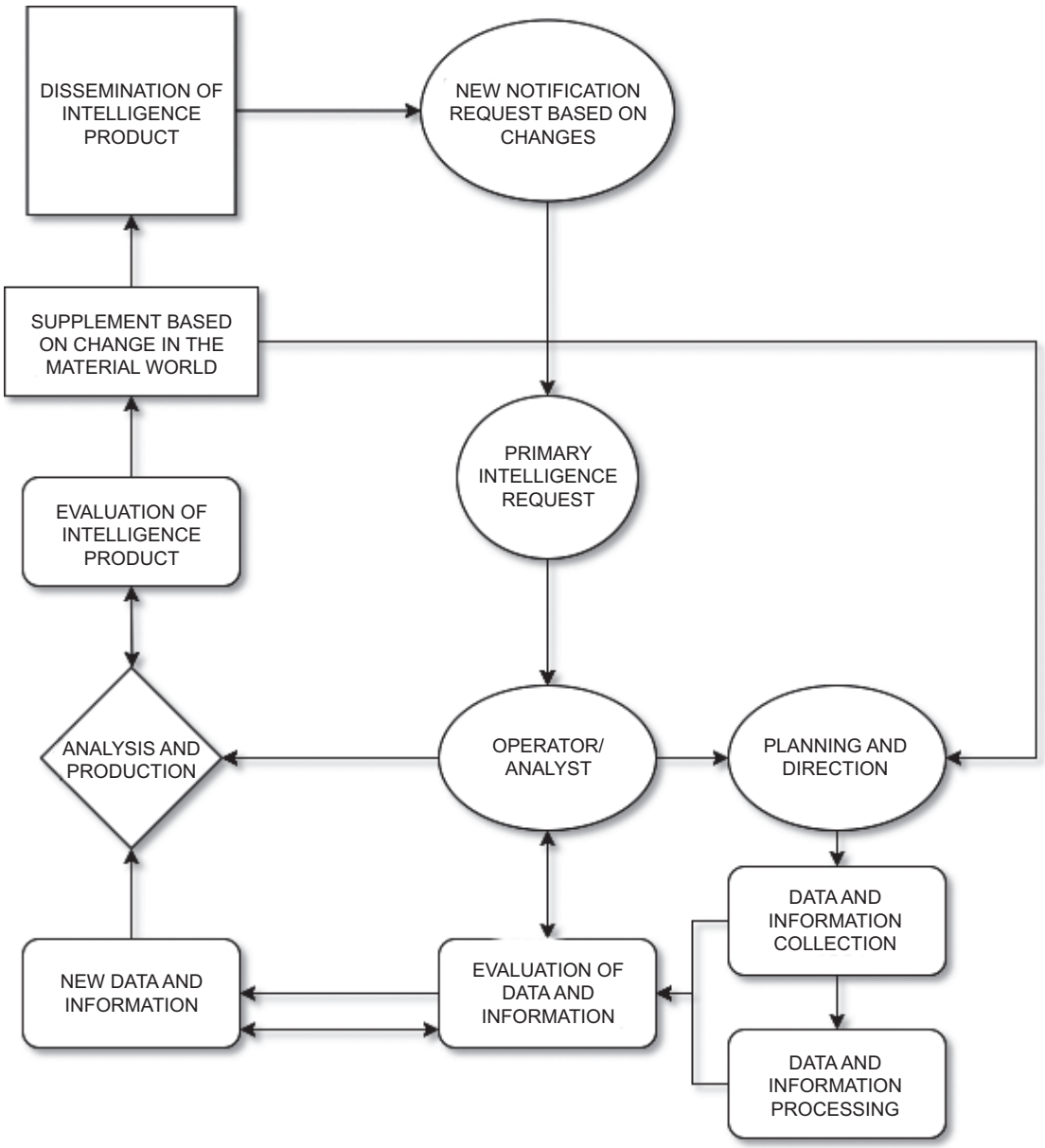

Figure 2. A simplified example of a redesigned intelligence cycle in a dynamic environment.

Transitioning to network-based models also comes with challenges and limitations. It requires a high level of coordination between different sectors and types of personnel; technical interoperability between systems and platforms; new communication protocols and an operational culture that supports flexibility and decentralisation; and a transformation of the analyst's role from a passive processor of data to an active participant in task development and

source prioritisation. This implies significant institutional reforms, including training analysts to think critically rather than mechanically, reducing dependence on technology alone, and fostering a culture of adaptability.

It is important to note that the idea of a network-based model is not entirely new – special units and intelligence teams operating in hostile territory have long used 'flat' structures instead of hierarchical linear models (e.g. Ukrainian SSO operating deep inside of Russian territories). What appears new today is the systematic effort to institutionalise this flexibility within large and complex organisations, such as national intelligence agencies. In the end, network models do not completely replace the traditional intelligence cycle. The classical model still has value for basic process structuring, especially in low-intensity situations. However, in modern operations, particularly in the context of special warfare – critics argue that the network approach can provide a more effective, realistic, and adaptable framework for producing and using intelligence.

Taken together, these elements highlight the emergence of what may be termed an *adaptive intelligence framework*. This framework rests on four dimensions: (a) simultaneity, where phases operate in parallel, rather than sequentially; (b) interactivity, with constant dialogue between analysts, operators, and decision-makers; (c) modularity, allowing sub-phases to be tailored to specific threats and contexts; and (d) resilience, ensuring redundancy and flexibility against disruption. By embedding these principles, intelligence work becomes less bound by rigid procedures and more attuned to the demands of special warfare, cyber threats, and hybrid operations, offering a potential bridge between analysis and action.

6. Operational Applicability in the Dynamic Environment of Special Warfare

Building on the transition towards adaptive and network-based intelligence models discussed in the previous section, many scholars and practitioners argue that their value becomes most visible in the operational domain of special warfare. Special warfare is, by its nature, multi-domain, multi-phase, and continuous, and its operations are designed based on strategic goals. A prominent example is China's 'three warfares' doctrine – psychological, media, and legal warfare, which has been systematically applied in the South China Sea disputes. Instead of relying solely on military strength, Beijing integrates legal claims (e.g. maritime jurisdiction), psychological pressure (e.g. intimidation of neighbouring states),

and media narratives (e.g. portraying island-building as defensive) into a continuous campaign. This demonstrates how special warfare transcends conventional battlefields, embedding itself simultaneously into political, informational, and legal domains, and illustrates the pressure on intelligence systems to adapt to this broadened scope.

Defending against actions carried out by enemy intelligence services or specific non-state actors (such as organised crime groups, terrorist organisations, or online activists under the control of those services) requires proper identification, classification, and neutralisation of threats. Critics argue that this is difficult to achieve through a traditional intelligence cycle understood in strictly linear terms. The philosophy behind special warfare is based on dynamic *ad hoc* exploitation of opportunities and long-term intelligence penetration and processing of various actors, institutions, and organisations. Such approaches complicate step-by-step intelligence models, since success often depends on improvisation, parallel action, and iterative adaptation rather than linear sequencing. This operational logic places enormous strain on analysts, who must process vast amounts of heterogeneous data and weave it into a coherent picture of the adversary's objectives. The concept of a war room that integrates all the relevant components of intelligence and operational systems in order to complete the intelligence and operations cycle in real time has become the standard way of thinking [16].

The phenomenon of cognitive overload illustrates this problem. Heuer [27] was one of the first to point out that, while a greater flow of information can potentially lead to deeper insights, it also brings the risk of losing focus, making incorrect interpretations, and delaying decision-making. This problem has been repeatedly highlighted in the US and NATO commission reports on intelligence reform, which warned that the exponential growth of digital information could overwhelm analytical systems if not properly managed [28]. The war in Ukraine vividly demonstrates this challenge as analysts face torrents of satellite imagery, intercepted communications, and millions of daily social media posts, many of which are deliberately manipulated to deceive. The resulting flood of both authentic and falsified data has created a constant risk of analytical paralysis, where critical warning signals risk being lost in the noise. In the 2022 Russian invasion of Ukraine, simultaneous cyberattacks, disinformation campaigns, military strikes, and economic disruptions placed enormous stress on linear intelligence cycles, while adaptive and network-based approaches were reported to provide greater flexibility in fusing fragmented data streams into actionable

insights. In modern special operations which often take place across several domains at the same time (cyber, informational, political, and economic), analysts are constantly under pressure to 'connect the dots' between fragmented, misleading, or deliberately contradictory data. In short, the clear line between collection and analysis is blurring. Slowly but surely all participants in the intelligence system are becoming partners in a shared process [16]. This makes it difficult to build an accurate analytical narrative, especially when it comes to recognising patterns that signal the presence of a sophisticated non-linear threat, such as special warfare. A clear example of this challenge is the Russian use of combined cyber and information operations against Ukraine.

During the 2014 annexation of Crimea and later the 2022 invasion, cyberattacks on government networks, media outlets, and critical infrastructure were closely synchronised with large-scale disinformation campaigns designed to paralyse decision-making and sow public confusion. These operations created overlapping waves of digital 'noise', where false narratives amplified through social media obscured the real operational objectives, while cyber intrusions disrupted communication channels at critical moments [28]. Disinformation, in particular, has proven to be a potent tool of geopolitical power competition and domestic political warfare, weaponising the fractured information environment and creating real-world effects. Sustained and well-funded campaigns, such as those pioneered by Russia and later adopted by China and Iran, rely on high-volume, multi-platform messaging often termed the 'firehose of falsehood' to deepen societal fissures, erode trust, and overwhelm cognitive resources [29].

What distinguishes contemporary special warfare, according to many analysts, is not that it introduces multi-domain threats for the first time but that digital technologies amplify their simultaneity, scale, and speed (see Fig. 2). It relies on continuous systematic penetration and processing of the target, whose control, destabilisation, or destruction serves a broader strategic objective. From this perspective, the traditional linear intelligence cycle, with its hierarchical bureaucracy, has limitations in fast-moving environments. The solution lies in designing the intelligence cycle as a network, where nodes communicate constantly, in multiple directions, and in real time. In this model, the decision-maker or the originator of the intelligence request actively participates in the process along with the operator or analyst, unlike in the traditional linear cycle. A compelling illustration of adaptive intelligence in practice is Israel's use of AI-enabled fusion centres. During the May 2021 Gaza conflict, a

senior colonel from Unit 8200 revealed that their team employed a form of 'data-science magic powder' to uncover previously unknown operativesby analysing social links and patterns, tens of thousands of potential targets were flagged as Hamas or Islamic Jihad affiliates, dramatically enhancing the speed and precision of targeting decisions [30]. This example highlights how adaptability can be institutionalised through permanent fusion centres and AI-enabled workflows, where analysis and operations are fused in real time, rather than improvised on a case-by-case basis. Unlike Clark's target-centric model [13], which centralises information around one target, this model is event-driven and contextual, enabling intelligence to evolve in response to unfolding developments (see Fig. 3). Similar principles were observed in Ukraine, where fusion cells of military officers, intelligence analysts, and cyber specialists worked together in real time to counter Russian advances. As the operational environment becomes more complex, driven by the adversary's strategy

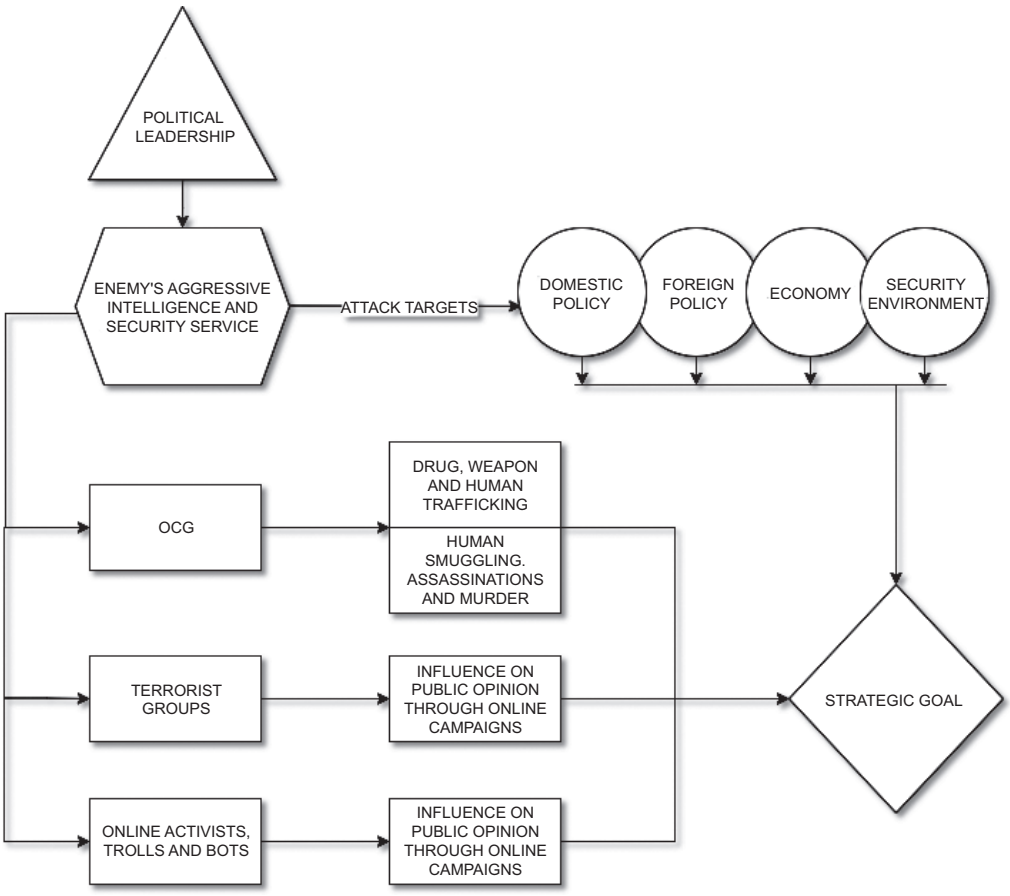

Figure 3. Multivector example of an attack to achieve a strategic goal.

and directly aligned with their goals, this demands greater dynamism, flexibility, and adaptability. If any of these elements is missing, the adversary may exploit the situation and carry out an *ad hoc* action that either supports long-term operations or becomes the foundation for launching a new one by penetrating intelligence systems and undermining the security structure.

In a complex operational environment, the strategic goal influences the operating environment, creating a need for intelligence information that will help make decisions (see Fig. 4). Analysts

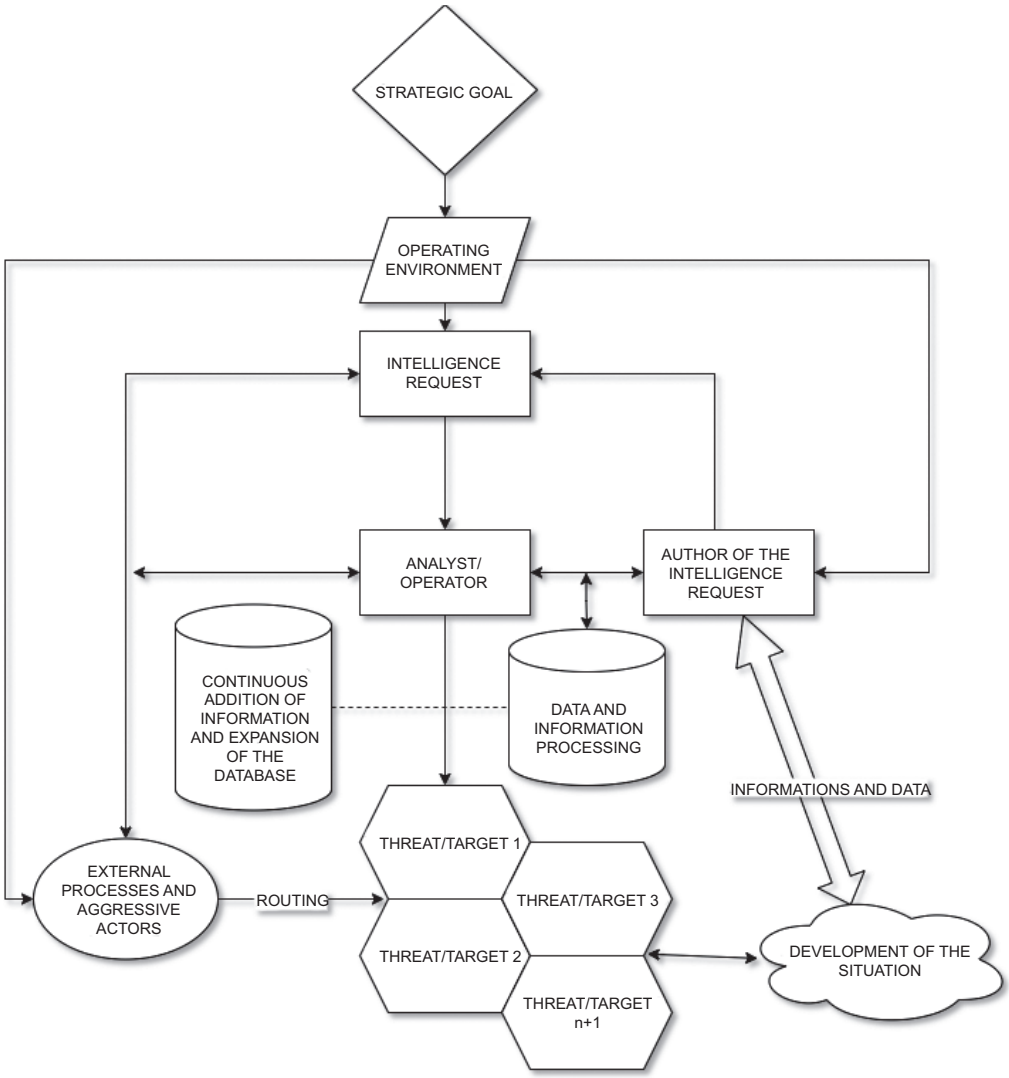

Figure 4. Dynamic environment and decision-making process.

and operators, with the help of continuously expanded databases and data processing, gather and process information to identify threats and targets, thus adapting to the dynamic intelligence cycle. Based on this analysis, the situation develops and information is routed within the organisation to establish a continuous and effective intelligence cycle that supports operations and achieves strategy. This shift underscores a deeper truth, the adversary constantly adapts, employing new methods of subversion. Since the state is usually the primary actor that initiates and directs special warfare [31], entities under its control ranging from intelligence services as executors to organised crime groups (OCGs), terrorist organisations, cyber activists, NGOs, and others, can be mobilised across both kinetic and non-kinetic domains. In practice, OCGs may be tasked with trafficking narcotics into a community, leading to widespread addiction and increased mortality; in parallel, hackers or cyber activists may target critical infrastructure to paralyse governance. The targeted state, unable to respond adequately, experiences reduced social cohesion and cascading destabilisation. Such dynamics have been visible in the Western Balkans and Moldova, where Russian-backed networks have exploited corruption, organised crime, and energy dependency as levers of geopolitical pressure. Declining cohesion and security then become an entry point for further operations, often supported by corrupt activities directed at political decision-makers. In this way, organised crime transforms into a tool of geopolitical penetration, and narcotics become one among many instruments for the systemic weakening of society's fabric.[2]

Beyond these cases, multi-phase and multi-domain campaigns where OCGs, assassins, cyber activists, terrorists, and hackers operate in overlapping waves create an intelligence problem of a higher magnitude. The diversity of actors and methods obscures the true objective of an operation, while the sheer volume of incoming data generates 'noise' that obstructs analysis. These conditions underscore why network-based intelligence must not only accelerate data processing but institutionalise adaptability itself. Mechanisms such as real-time fusion centres, cross-domain task forces, and dynamic prioritisation frameworks can help mitigate cognitive overload, turning analysts and decision-makers into joint participants in a live, iterative process that mirrors the actual tempo of special warfare.

Some analysts go as far as to argue that the transition towards adaptive intelligence models is not merely a theoretical preference but an operational necessity imposed by the dynamics of modern

[2]The above example closely correlates with the drug crisis occurring in the southern United States. Mexican cartels that use Chinese precursors to make fentanyl are often contaminated and cause high mortality. The People's Republic of China played a key role in the early phase of fentanyl crisis, since the first large quantities of fentanyl and its analogues that arrived at the illegal market in the United States (2013–2014) originated precisely from China [32]. This dynamics indicate the adaptability and complexity of low-intensity special warfare conducted through narcotics and financial flows, where the country of origin of the precursors and financial channels may not necessarily be directly responsible, but is a key intermediary in the destabilisation of another state. From the perspective of special warfare, China seeks to cause social anomie, distrust in state institutions, and disrupt social cohesion through long-term operations involving OCG, which can have serious political consequences.

conflict. Embedding flexibility, resilience, and cross-domain integration into intelligence work offers a pathway to countering the persistence and sophistication of contemporary adversaries. Yet it simultaneously raises a fundamental dilemma -- how can these adaptive models be institutionalised without eroding coherence, accountability, or strategic focus? One possible answer lies in hybrid governance frameworks that combine decentralised operational flexibility with centralised oversight mechanisms. Operational lessons from the United States and NATO demonstrate this principle. During operations in Iraq and Afghanistan, interagency fusion cells that integrated all-source analysts with technical collection assets proved decisive in accelerating decision-making and disrupting adversary networks [33].

For instance, real-time fusion centres may be granted autonomy to adapt methods and priorities in response to fluid threats, while independent auditing bodies and parliamentary oversight committees preserve accountability and transparency. Another avenue involves embedding adaptability into doctrine and training, ensuring that flexibility is not improvised but systematically taught, rehearsed, and evaluated through red-teaming and stress-testing exercises. Digital solutions – such as machine learning-assisted triage systems can further reduce cognitive overload by filtering and prioritising intelligence flows without replacing human judgement. Contemporary practice illustrates this balance. The US Department of Defense's Joint All-Domain Command and Control (JADC2) initiative seeks to integrate sensors, shooters, and decision-makers across land, sea, air, cyber, and space domains in near-real time, thereby institutionalising adaptability without abandoning centralised command authority [34]. Similarly, the United Kingdom established the National Situation Centre in 2021 to provide 24/7 data-driven monitoring and crisis response capabilities, embedding flexibility within a formal structure directly accountable to the Cabinet Office [35]. Addressing this tension between adaptability and governance forms the subject of the next section, which examines the structural and organisational implications of intelligence reform in the age of special warfare.

7. Operationalising the Network Model of Intelligence Cycle

Having examined the conceptual foundations and governance dilemmas of adaptive intelligence models in the previous section, this section turns to the question of practice: how elements of the network model of the intelligence cycle can be translated

from theory into concrete institutional, procedural, and technological reforms? The transformation of an intelligence cycle from a linear to a network model is often described not as a complete replacement but as a gradual adaptation that must be grounded in institutional practice. As discussed in the context of special warfare operations, critics argue that only approaches which are simultaneously adaptive and integrated can respond effectively to hybrid threats. In this context, operationalisation means developing capacity, implementing appropriate protocols, and adapting organisational culture and technical systems to support a simultaneous, dynamic, and multidirectional intelligence process. At the institutional level, building a functional network model requires intelligence services to move away from strictly hierarchical processes and organisational logic.

It is necessary to establish the so-called 'flat' operational structures in which analysts, operators, and decision-makers work together in real time through joint operational centres or digital collaborative platforms. However, the operationalisation of the network model is not without risks. The very features that make it dynamic-simultaneity, decentralisation, and constant feedback – can also generate vulnerabilities. For instance, while real-time sharing enhances responsiveness, it also magnifies the risk of information saturation and analytical noise. Another development that has challenged the validity of the intelligence cycle is the creation of a networked log shared by all parties, which in wartime allows all participants to provide and receive updates in real time [16]. Networked intelligence processes are more exposed to information saturation, where the rapid circulation of unverified data may amplify noise instead of clarity. Decentralised structures can indeed foster agility, yet they also risk diluting accountability and complicating the assignment of responsibility for failures. For example, NATO after-action reviews of Afghanistan operations highlighted that interagency fusion centres not only accelerated tactical decision-making but also generated ambiguity regarding command responsibility [33]. Moreover, the emphasis on real-time analysis and decision-making increases the danger of premature conclusions, privileging speed over depth. From a counterintelligence perspective, the interconnected nature of network models multiplies the potential attack surfaces for adversarial infiltration or disinformation campaigns. For these reasons, many authors stress that institutionalising the network model requires not only technical integration but also safeguards that preserve analytical rigour, secure communication channels, and clear lines of authority. Without such measures, the promise of adaptability risks collapsing into fragmentation and

systemic vulnerability. Yet, these vulnerabilities should not be seen as arguments against the network model, but rather as reminders that adaptability must always be coupled with robust counterintelligence and governance mechanisms. Accordingly, the role of leadership shifts from vertical control to a more mentorship – and facilitation-based function within the intelligence team. This institutional shift must be mirrored by a parallel technological transformation, since even the most flexible organisational design cannot function without interoperable digital systems that enable constant information flow.

From a technical perspective, operationalising the network model requires the integration of interoperable digital platforms that enable real-time data exchange, joint source analysis, collaborative scenario modelling, and metadata visualisation using dynamic maps and graphs. Tools that combine big data analytics, predictive learning (ML/AI), and interactive visualisation become the foundation of daily operations.

Personnel transformation also plays a crucial role. In the network model, analysts are no longer passive recipients of data, they become active participants in threat identification and in designing operational responses. In short, the clear line between collection and analysis is blurring. As Siman-Tov and Ofer [16] suggests, participants across the system increasingly function as partners in a shared task. This requires changes in both training and recruitment. Instead of privileging narrow technical specialisation alone, intelligence services must cultivate interdisciplinary skill sets that combine analytical thinking under uncertainty; cultural and sociopolitical awareness; cognitive agility and the ability to manage information overload, and systems thinking that connects military, economic, and informational dimensions of special warfare. Training programmes should move away from static curricula towards continuous learning ecosystems that include scenario-based simulations, red teaming exercises, and stress testing of analytical assumptions. Recruitment strategies, meanwhile, must expand beyond traditional profiles to include expertise from data science, behavioural psychology, media studies, and even design thinking disciplines that strengthen adaptability in complex hybrid environments. A practical illustration of this approach can be found in the US National Counterterrorism Center (NCTC), which has long relied on fusion cells staffed by personnel from the CIA, FBI, NSA, Department of Defense, and State Department. As officially defined, 'a fusion center is a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with

the goal of maximising their ability to detect, prevent, investigate, and respond to criminal and terrorist activity' [36]. These cells not only integrate technical and operational expertise but also employ social scientists and regional experts, ensuring that situational assessments incorporate both quantitative data and cultural context. Similarly, NATO's red-teaming initiatives have institutionalised interdisciplinary challenge sessions, bringing together intelligence officers, academics, and private-sector specialists to systematically test operational assumptions under stress [37]. At the regional level, Bosnia and Herzegovina has established a Joint Risk Analysis Center related to state border management. This centre, housed within the Border Police of BiH, brings together representatives of the Service for Foreigners' Affairs, the Indirect Taxation Authority, the Veterinary Office, and the Plant Health Administration. Its mandate is to produce joint annual risk assessments that serve as the foundation for management, organisation, and planning of operational activities [38].

Unlike the traditional model, where feedback appears only after the full cycle is completed, the network model treats feedback as a constant component. Every new piece of information is immediately redistributed across the network, enabling iterative corrections of analysis, redefinition of targets, and adjustment of operations, similar to the logic behind Clark's [13] target-centric approach. What distinguishes the network model from its linear predecessor is not only speed but also the permanent embedding of feedback, which transforms intelligence from a cycle into what some describe as a 'living process'. This continuous feedback loop has already been institutionalised in practice through mechanisms such as NATO's Federated Mission Networking, which allows member states to share intelligence updates in near real time, or through the European Union's Integrated Political Crisis Response (IPCR) system, which redistributes new information simultaneously across political, intelligence, and operational nodes [39, 40].

8. Examples of Use of Adaptive Intelligence Cycle in Complex Environments

The transition from a linear to an adaptive intelligence cycle is not only a conceptual innovation but also a practical necessity in operational environments characterised by simultaneity, deception, and hybrid threats. In order to demonstrate how adaptive principles can be applied in practice, this section presents several hypothetical illustrative scenarios. These examples are designed for analytical purposes only, and any resemblance

to actual events, actors, or operations is purely coincidental. Each scenario highlights the difference between rigid, sequential procedures, and network-based approaches that enable real-time integration of collection, analysis, and operational decision-making.

8.1. Countering Organised Crime Groups in Migrant Smuggling (Serbia–Bosnia and Herzegovina border)

Organised crime groups engaged in migrant smuggling operate across porous borders, combining local facilitators, regional coordinators, and transnational financial flows. A traditional intelligence cycle would require formal requests, phased collection, and delayed analysis. In contrast, an adaptive approach relies on simultaneity.

Parallel collection and planning: Border police, customs, and the Service for Foreigners' Affairs simultaneously collect HUMINT from intercepted migrants, SOCMINT from Telegram, WhatsApp, and Facebook groups advertising crossings, and technical data from drones, thermal cameras, and IMSI catchers.

Fusion and joint analysis: Analysts, investigators, and operators work together in a digital fusion centre, visualising smuggling routes, cross-border telephone links, and suspicious financial transfers. AI-assisted link analysis immediately flags overlapping patterns, for example, a single coordinator number connected to multiple groups.

Dynamic dissemination: Instead of static reports, interactive maps and real-time alerts are shared with mobile border patrols, allowing immediate operational response.

Continuous feedback: Each operational result, such as the interception of a smuggling vehicle, is instantly reintegrated into the system, updating maps and adjusting patrol routes. Intelligence thus becomes a 'living process', rather than a finished product.

While the narrative example illustrates how an adaptive intelligence cycle operates in practice, its comparative advantages become even clearer when contrasted with the limitations of the traditional cycle. Table 1 summarises key differences across the main phases of intelligence work, highlighting how adaptive principles provide greater speed, integration, and operational relevance in addressing migrant smuggling networks along the Serbia–Bosnia and Herzegovina border.

Table 1. Comparison of traditional vs. adaptive intelligence cycle in countering migrant smuggling OCGs (Serbia–Bosnia and Herzegovina border).

Phase/ function	Traditional intelligence cycle	Adaptive intelligence cycle
Planning and collection	Sequential: formal requests precede collection; delays in acquiring HUMINT/ SOCMINT; reliance on limited technical means.	Parallel: HUMINT from migrants, SOCMINT from Telegram/WhatsApp/Facebook, and technical data (drones, thermal cameras, IMSI catchers) gathered simultaneously.
Analysis	Isolated analytical cells produce reports after collection ends; limited integration with field operators.	Fusion centres integrate analysts, investigators, and operators in real time; AI-assisted link analysis reveals hidden patterns immediately.
Dissemination	Static reports circulated through bureaucratic channels; time lag reduces operational utility.	Dynamic: interactive maps and instant alerts transmitted to mobile border patrols; intelligence directly drives field action.
Feedback	Limited and delayed: feedback only after completion of full cycle; weak adaptability to fast-changing smuggling tactics.	Continuous: every interception or incident reintegrated into the system; patrols and analysis adapt routes and strategies in real time.
Overall effectiveness	Rigid, linear, and slow; prone to missing fluid cross-border activities.	Flexible, networked, and iterative; intelligence becomes a 'living process' that aligns with the tempo of criminal networks.

The table highlights that traditional intelligence cycles, with their linear sequencing and delayed feedback, struggle to keep pace with fluid cross-border criminal activity. In contrast, the adaptive model leverages simultaneity, joint analysis, and real-time dissemination to transform intelligence into an operational tool. This continuous loop ensures that every new interception strengthens the overall system, allowing security services to respond proactively, rather than reactively to organised crime networks.

8.2. Special Operations Behind Enemy Lines

Unnamed Special Operations Forces are operating deep inside enemy territory face conditions where rigid planning collapses under the weight of uncertainty and simultaneity. The discovery of a critical infrastructure target during movement demands immediate adaptation. Instead of relying on a sequential cycle, the adaptive approach enables real-time decision-making and operational flexibility:

Simultaneous reconnaissance and planning: While preparing for an initial mission, the SOF team unexpectedly encounters a vulnerable segment of enemy critical infrastructure (e.g. power substation or railway junction). HUMINT from local contacts, combined with

real-time UAV reconnaissance and SIGINT intercepts, immediately feeds into the planning cell.

Fusion and operational analysis: A small mobile fusion node within the team integrates tactical data, enemy patrol patterns, and environmental conditions. Analysts embedded with the unit provide on-the-spot risk assessment, while headquarters remotely validates potential strategic impact.

Dynamic dissemination and execution: Updated intelligence is transmitted directly to demolition experts and assault elements in real time. Instead of waiting for formal approval through hierarchical channels, mission parameters are refined on the move, enabling rapid deployment of explosives and tactical diversionary measures.

Continuous feedback and adaptation: As the sabotage unfolds, incoming drone imagery and SIGINT alerts are fed back into the system, allowing the team to adjust escape routes or counter incoming reinforcements. Intelligence thus becomes an iterative loop between operators, embedded analysts, and remote command, ensuring survivability and mission success in an unplanned scenario.

This scenario demonstrates the urgency of adaptive intelligence in high-risk environments, where unexpected opportunities demand immediate exploitation. To better understand why the adaptive cycle outperforms the traditional model in such contexts, Table 2 contrasts both approaches across the main intelligence phases. It highlights how simultaneity, real-time feedback, and decentralised decision-making directly translate into operational success for SOF units operating behind enemy lines.

This comparison underscores that traditional intelligence cycles, with their dependence on sequential planning and hierarchical approval, are fundamentally mismatched to the tempo of special operations behind enemy lines. By embedding simultaneity, rapid dissemination, and continuous feedback, the adaptive cycle transforms intelligence into a living process that directly supports survivability and mission success under highly uncertain and fluid conditions.

8.3. Detecting a Foreign Intelligence Cell Operating Domestically

Foreign intelligence services often establish small, compartmentalised cells that blend into the local environment while

Table 2. Comparison of traditional vs. adaptive intelligence cycle in special operations.

Phase/function	Traditional intelligence cycle	Adaptive intelligence cycle
Planning and collection	Sequential tasking; targets identified before mission; limited ability to respond to unforeseen opportunities.	Simultaneous reconnaissance and planning; HUMINT, UAV, and SIGINT data integrated in real time when new targets emerge.
Analysis	Conducted away from the field, often delayed; risk of information becoming outdated before reaching operators.	Embedded analysts and mobile fusion cells provide instant risk assessments; HQ validates impact remotely without disrupting tempo.
Dissemination and execution	Hierarchical approval needed before mission adjustments; delays can compromise surprise or mission feasibility.	Intelligence directly disseminated to demolition teams and assault elements; mission parameters refined dynamically during execution.
Feedback	Occurs only after completion of mission; minimal impact on live decision-making.	Continuous: drone imagery and SIGINT alerts loop back immediately, updating escape routes and countering enemy reactions.
Overall effectiveness	Rigid, slow, and unsuitable for fluid battlefield conditions; prone to mission failure if circumstances change.	Flexible, iterative, and resilient; intelligence becomes a 'living process' that ensures survivability and operational success in *ad hoc* sabotage.

conducting recruitment, surveillance, or sabotage. A rigid intelligence cycle, with its delayed analysis and sequential processing, risks missing the fleeting indicators of such covert activity. An adaptive approach, however, allows for rapid exposure and disruption.

Parallel detection and collection: Domestic security services simultaneously exploit multiple sources – HUMINT from local informants, SOCMINT from suspicious online contacts, financial intelligence (unexplained transfers), and SIGINT intercepts of encrypted communications. Instead of waiting for formal tasking, collection streams run continuously and in parallel.

Fusion and pattern recognition: Analysts, counterintelligence officers, and cyber specialists collaborate in a joint fusion cell. Real-time link analysis integrates the movements, communications, and financial transactions of six suspected members, revealing shared safe houses and overlapping contact points.

Dynamic dissemination and operational response: Rather than issuing lengthy intelligence products, operational alerts are pushed instantly to surveillance teams and tactical units. This enables synchronised monitoring of the entire network, preventing suspects from dispersing or destroying evidence once initial detection occurs.

Continuous feedback and escalation: Each new interception, for example, the capture of a courier or confiscation of digital storage is immediately reintegrated into the system. Analytical nodes update adversary profiles and refine assessments of the cell's objectives, allowing decision-makers to escalate from monitoring to neutralisation without delay.

The detection of clandestine intelligence cells is among the most time-sensitive and complex counterintelligence tasks. Traditional models, with their delayed responses and sequential procedures, often fail to identify weak signals before they escalate into significant threats. By contrast, the adaptive cycle enables simultaneous data flows, integrated analysis, and rapid operational responses. Table 3 compares both approaches, emphasising the strengths of adaptive intelligence in neutralising a six-member foreign cell operating domestically.

The contrast demonstrates that while a traditional cycle risks paralysis through delay and compartmentalisation, an adaptive model ensures rapid integration of multi-source data and immediate operational response. By treating intelligence as an iterative and networked process, security services are better positioned to expose, disrupt, and neutralise hostile cells before they consolidate or achieve their objectives.

Table 3. Comparison of traditional vs. adaptive intelligence cycle in detecting a foreign intelligence cell.

Phase/function	Traditional intelligence cycle	Adaptive intelligence cycle
Detection and collection	Relies on formal tasking and sequential collection; delays may miss early indicators of covert activity.	Parallel exploitation of HUMINT, SOCMINT, financial intelligence, and SIGINT; streams run continuously and adaptively.
Analysis	Isolated analysts evaluate data after collection; compartmentalisation slows identification of links.	Fusion cells combine analysts, counterintelligence officers, and cyber specialists; real-time link analysis reveals networks and safe houses.
Dissemination and response	Reports circulated through hierarchical channels; lag reduces ability to prevent cell dispersion or evidence destruction.	Instant operational alerts sent to surveillance and tactical teams; synchronised monitoring disrupts adversary activity in real time.
Feedback	Feedback gathered post-operation, often too late to inform ongoing counterintelligence action.	Continuous integration of new interceptions (e.g. courier capture, digital media analysis) refines adversary profiles and escalates responses.
Overall effectiveness	Linear, reactive, and vulnerable to deception; risks allowing cell consolidation before intervention.	Iterative, proactive, and resilient; intelligence becomes a 'living process' that ensures rapid exposure and disruption of covert networks.

8.4. Cyber Attack on Critical Infrastructure

Critical infrastructure, such as energy facilities, represents one of the most attractive targets for cyber operations, as even temporary disruption can have strategic, political, and psychological effects. A traditional intelligence cycle, with its reliance on sequential collection and delayed analysis, is ill-suited for the speed and simultaneity of cyberattacks. An adaptive model, however, provides the resilience and agility necessary to detect, analyse, and counter hostile operations in real time.

Simultaneous detection and collection: Security operation centres (SOCs), SIGINT units, and private-sector IT partners monitor intrusion attempts in parallel. Indicators of compromise from phishing emails, DDoS traffic, and malware signatures are immediately shared across agencies.

Fusion and collaborative analysis: Analysts from cyber intelligence units, plant engineers, and law enforcement work together in a digital fusion cell. Real-time correlation of network logs, malware behaviour, and physical system responses (e.g. turbine sensors) identify whether the attack is limited to IT systems or already affecting operational technology (OT).

Dynamic dissemination and operational response: Alerts are transmitted instantly to both plant operators and national cyber defence units. Countermeasures, such as isolating infected segments, activating backup systems, and deploying traffic filters, are implemented within minutes, while intelligence flows continue uninterrupted.

Continuous feedback and resilience: Every detected intrusion or blocked exploit is reintegrated into the system, improving threat intelligence databases and predictive models. Lessons learned are immediately applied to strengthen defensive posture, ensuring resilience against follow-up attacks.

Cyberattacks against thermal power plants illustrate how linear intelligence cycles lag behind the tempo of digital threats, where milliseconds can determine success or failure. Table 4 contrasts traditional and adaptive models, emphasising how simultaneity, fusion, and continuous feedback directly enhance resilience in the protection of critical infrastructure.

This comparison demonstrates that defending critical infrastructure from cyberattacks requires more than traditional sequential

Table 4. Comparison of traditional vs. adaptive intelligence cycle in cyber defence of a thermal power plant.

Phase/function	Traditional intelligence cycle	Adaptive intelligence cycle
Detection and collection	Sequential log review and incident reporting; delays in recognising coordinated attacks.	Simultaneous monitoring by SOCs, SIGINT, and private IT partners; indicators of compromise shared in real time.
Analysis	Conducted in isolation after incidents; difficulty linking IT and OT data.	Fusion centres integrate cyber analysts, plant engineers, and law enforcement; real-time correlation of network and sensor data.
Dissemination and response	Reports passed through bureaucratic channels; delayed operational reaction may allow attacker persistence.	Instant alerts delivered to plant operators and national cyber defence teams; countermeasures executed immediately.
Feedback	Lessons learned compiled post-incident; slow integration into future defences.	Continuous reintegration of intrusion data into predictive models; resilience enhanced with every new attempt.
Overall effectiveness	Reactive, rigid, and prone to critical delays; high risk of operational disruption.	Proactive, iterative, and resilient; intelligence becomes a living process that ensures continuity of critical infrastructure.

intelligence processes. By embedding simultaneity, cross-domain fusion, and continuous feedback, the adaptive cycle transforms cyber defence into a resilient, real-time process. In the context of a thermal power plant, such adaptability can mean the difference between temporary disturbance and prolonged national-scale blackout.

9. Conclusions

The modern security environment is marked by the rise of unconventional threats that appear not only in the physical world but also increasingly in abstract domains, such as informational, psychological, economic, cyber, and political. In this context, many analysts argue that special warfare represents one of the defining forms of contemporary conflict, with characteristics that put sustained pressure on the institutional and operational capacities of intelligence services. At the same time, completely *ad hoc* approaches where key phases are skipped risk leading to operational unreliability, misinterpretation, and strategically harmful decisions. Between these two extremes lies the need for a model that offers flexibility, speed, and adaptability, while still preserving analytical depth and institutional coordination.

One proposed response is the operationalisation of a network-based intelligence cycle, understood as a framework that enables

continuous communication and the simultaneous execution of key functions, from data collection and analysis to dissemination and feedback. In such a model, the decision-maker becomes an integral part of the intelligence process, reducing the time gap between threat detection and political response. This is especially important in foreign policy contexts, where multiple actors, interests, and parallel processes shape the operational space. A missing link in the intelligence chain – whether it is the analyst, operator, supervisor, or strategic decision-maker – can lead to a serious misunderstanding of the true nature of the threat. Unlike the traditional model, the network model is presented as enhancing resilience through multidirectional communication, task decentralisation, and constant real-time data updates. However, operationalising this approach requires more than conceptual innovation: it demands doctrinal adjustments, the development of interoperable technical platforms, and sustained investment in training programmes that cultivate cognitive agility, interdisciplinary expertise, and collaborative leadership. At the same time, safeguards must ensure that decentralisation does not erode accountability, and that flexibility does not come at the expense of analytical rigour. Examples from international practice point in this direction through NATO's Federated Mission Networking, the EU's Integrated Political Crisis Response mechanism, and the proliferation of national fusion centres, suggesting that the shift towards more networked intelligence processes is both feasible and adopted increasingly.

For these reasons, the implementation of network-inspired approaches to the intelligence cycle should be seen not as an optional experiment but as part of an ongoing transformation in how intelligence communities think, act, and produce knowledge in complex environments. This model is not merely a tool for adaptation, but also a means for proactively shaping the security environment and maintaining strategic stability in an era of heightened multi-domain threats. Ultimately, embracing networked approaches may help intelligence organisations sustain analytical credibility and strategic relevance, although this evolution must remain balanced with oversight, accountability, and methodological rigour.

References

[1] N. Gažević, *Vojna enciklopedija*, vol. 9. Beograd: Vojnoizdavački zavod, 1975.

[2] B. Mamula, *Odbrana malih zemalja*. Beograd: VIZ i Novinski Centar, 1988.

[3] North Atlantic Treaty Organization (NATO), *Allied joint doctrine for special operations (AJP-3.5)*. Brussels: NATO, 2019.

[4] R.N. McDermott and C.K. Bartles, "Defining the 'Special Military Operation'," *NATO Defense College*, Mar. 28, 2022. [Online]. Available: https://www.ndc.nato.int/news/news.php?icode=1650. [Accessed: May 11, 2025].

[5] Defense Intelligence Agency (DNI), *Terms & definitions of interest for DoD counterintelligence professionals*. Washington, DC: DNI, 2011.

[6] D.F. O'Leary, *Approaching career criminals with an intelligence cycle*. Monterey, CA: Naval Postgraduate School, 2015.

[7] J. Goldman, *Words of intelligence: An intelligence professional's lexicon for domestic and foreign threats*. Lanham, MD: Scarecrow Press, 2011.

[8] Central Intelligence Agency (2024). *The intelligence cycle*, 2024. [Online]. Available: https://www.cia.gov/spy-kids/static/59d238b4b5f69e0497325e49f-0769acf/Briefing-intelligence-cycle.pdf. [Accessed: May 12, 2025].

[9] K.L. Petersen ,V.S. Tjalve, "Intelligence expertise in the age of information sharing: Public–private 'collection' and its challenges to democratic control and accountability," *Intelligence and National Security*, vol. 32, no. 1, pp. 21–35, 2017. doi: 10.1080/02684527.2017.1316956

[10] A.S. Hulnick, "What's wrong with the intelligence cycle," *Intelligence and National Security*, vol. 21, no. 6, pp. 959–979, 2006, doi: 10.1080/02684520601046291.

[11] G. Evans, "Rethinking military intelligence failure – Putting the wheels back on the intelligence cycle," *Defence Studies*, vol. 9, no. 1, pp. 22–46, 2009. doi: 10.1080/14702430701811987.

[12] P.H. Davies, K. Gustafson, I. Rigden, "The intelligence cycle is dead, long live the intelligence cycle: Rethinking intelligence fundamentals for a new intelligence doctrine," in *Understanding the intelligence cycle*, M. Phythian, Ed. London: Routledge, 2013, pp. 56–76.

[13] R.M. Clark, *Intelligence analysis: A target-centric approach*, 5th ed. Washington, DC: CQ Press, 2016.

[14] D. Kilcullen, *The dragons and the snakes: How the rest learned to fight the west*. Oxford: Oxford University Press, 2020.

[15] M.M. Lowenthal, *Intelligence: From secrets to policy*, 7th ed. Washington, DC: CQ Press, 2017.

[16] D. Siman-Tov, G. Ofer, "Intelligence 2.0: A new approach to the production of intelligence," *Military and Strategic Affairs*, vol. 5, no. 1, pp. 31–51, 2013.

[17] D. Korać, "Obavještajni ciklus u obavještajnim agencijama," *Kriminalističke teme*, vol. 10, no. 1–2, pp. 79–97, 2010.

[18] M. Warner, "The past and future of the intelligence cycle," in *Understanding the intelligence cycle*, M. Phythian, Ed. London: Routledge, 2013, pp. 9–20.

[19] Galeotti, M. (2019). *Active measures: Russia's covert geopolitical operations* (No. 031). George C. Marshall European Center for Security Studies. Available: https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0(Accessed [Accessed: May 17, 2025].

[20] T. Rid, *Active measures: The secret history of disinformation and political warfare*. New York, NY: Farrar, Straus and Giroux, 2019.

[21] K. Takagi (Jul. 22, 2022). The future of China's cognitive warfare: Lessons from the war in Ukraine, *War on the Rocks*. [Online]. Available: https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/. [Accessed: Jul. 13, 2025].

[22] R. Morris, "What are the shortcomings of the Intelligence Cycle and how might they be mitigated?" *Tac Talks*. [Online]. Available: https://tactalks.co.uk/shortcomings-intelligence-cycle [Accessed: Aug. 24, 2025].

[23] N. Krohley (Oct. 24, 2017). The intelligence cycle is broken. Here's how to fix it, *Modern War Institute*. [Online]. Available: https://mwi.westpoint.edu/intelligence-cycle-broken-heres-fix/. [Accessed: Aug. 08, 2025].

[24] P. Gill, M. Phythian, "From intelligence cycle to web of intelligence: Complexity and the conceptualisation of intelligence," in *Understanding the intelligence cycle*, M. Phythian, Ed. London: Routledge, 2013, pp. 21–42.

[25] A. Dinerman (Nov. 18, 2015). "SOF–GPF integration: A model for cyber operations," *The Cyber Defense Review* [Online]. Available: https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136040/sof-gpf-integration-a-model-for-cyber-operations. [Accessed: Aug. 17, 2025].

[26] R. Johnston, *Analytic culture in the US intelligence community*. Washington, DC: Center for the Study of Intelligence, 2005.

[27] R.J. Heuer, *Psychology of intelligence analysis*. Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 1999.

[28] US Government, Senate Select Committee on Intelligence, *Russian active measures campaigns and interference in the 2016 US election, Vol. 1–5*. Washington, DC: US Government Publishing Office, 2020.

[29] K. Sedova, C. McNeill, A. Johnson, A. Joshi, I. Wulkan, *AI and the future of disinformation campaigns*. Washington, DC: Center for Security and Emerging Technology (CSET), 2021.

[30] H. Davies, B. McKernan (Apr. 22, 2024). IDF colonel discusses 'data science magic powder' for locating terrorists, *The Guardian*. [Online]. Available: https://www.theguardian.com/world/2024/apr/11/idf-colonel-discusses-data-science-magic-powder-for-locating-terrorists. [Accessed: Aug. 01, 2025].

[30] North Atlantic Treaty Organization (NATO), *Allied joint doctrine for special operations*. Brussels: NATO, 2013.

[31] E. Muhić, *Teoretsko-metodološki aspekti specijalnog rata,* doctoral dissertation. Sarajevo: Fakultet za kriminalistiku, Kriminologiju I Sigurnosne Studije, UNSA, 2025.

[32] V. Felbab-Brown (Oct. 1, 2024). The fentanyl pipeline and China's role in the US opioid crisis, *Brookings Institution*. [Online]. Available: https://www.brookings.edu/articles/the-fentanyl-pipeline-and-chinas-role-in-the-us-opioid-crisis/. [Accessed: May 21, 2025].

[33] L. Robinson, P.D. Miller, J. Gordon, J. Decker, M. Schwille, R.S. Cohen, *Improving strategic competence: Lessons from 13 years of war*. Santa Monica, CA: RAND Corporation, 2015.

[34] Department of Defense (DoD), *Summary of the joint all-domain command and control (JADC2) strategy*. Washington, DC: DoD, 2022.

[35] H.M. Government, UK, *The Amber book: Managing crisis in central government*. London: Cabinet Office Briefing Rooms, 2025.

[36] US Department of Homeland Security and US Department of Justice, *Fusion center guidelines: Developing and sharing information and intelligence in a new era*. Washington, DC: DHS and DoJ, 2006.

[37] L. Dandurand, "Rationale and blueprint for a cyber red team within NATO: An essential component of the alliance's cyber forces," in *Proceedings of the 3rd International Conference on Cyber Conflict*, Tallinn, Estonia, 2011, pp. 71–86.

[38] Council of Ministers of Bosnia and Herzegovina, *Strategy for integrated border management in Bosnia and Herzegovina for the period 2025–2029*. Sarajevo: Council of Ministers of BiH, 2025.

[39] I.D. Beriain, E. Atienza-Macías, E.A. Armaza, "The European Union integrated political crisis response arrangements: Improving the European Union's major crisis response coordination capacities," *Disaster Medicine and Public Health Preparedness*, vol. 9, no. 3, pp. 234–238, 2015, doi: 10.1017/dmp.2015.10.

[40] North Atlantic Treaty Organization (NATO) (2025). NATO allied command transformation, *Federated Mission Networking*. [Online]. Available: https://www.act.nato.int/activities/federated-mission-networking. [Accessed: Sept. 03, 2025].

[42] United States Marine Corps, *MCWP 2-10: Intelligence operations*. Washington, DC: USMC, 2021.