The 17th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, October 28th-29th 2021

HOW THE SECRET INTELLIGENCE SERVICES WILL CHANGE AFTER THE RUSSIA – UKRAINE WAR

PĂIUȘ Ioana Hermina

PhD candidate Babeș Bolyai University Cluj-Napoca, Romania

Abstract:

Intelligence has changed. Secret Services is no longer just about spying or passively watching a target. Espionage chiefs now command secret armies and legions of cyber warriors who can quietly shape international relations itself. Intelligence actively supports diplomacy, peacekeeping and warfare: the entire spectrum of security activities. As traditional interstate wars become more costly, covert action, black propaganda and other forms of secret interventionism become more important. This ranges from proxy warfare to covert action; from targeted killing to disruption activity. Meanwhile, surveillance permeates communications to the point where many feel there is little privacy. Intelligence, and the accelerating technology that surrounds it, have never been more important for the citizen and the state. We will examine: why states choose to use intelligence – including fabricated intelligence for influencing external audiences, the different methods they deploy for doing so, the gains and costs of publicising intelligence, and how open-source third-parties affect this and, therefore, how the use of intelligence during the Russia-Ukraine conflict should be understood within broader historical and contemporary trends. We conclude that while liberal democracies' use of intelligence in public is to be welcomed, this will need careful risk management - from sources and methods to public trust and politicization- if it is to become a new normal of statecraft moving forward.

Key words: Intelligence; invasion; Ukraine; Russia; consequences; secret; change; war.

1. Introduction

It is no secret that the use of technology has revolutionized our way of everyday life last few decades. We are, in the modern world, all connected to each other and to society through the use of cyberspace and information technology, in various ways. This revolutionizing change is also present in conflicts, within channels for diplomacy and modern war. Historically, conflicts have adapted the arena of conflict through various means of innovations and inventions, from land to ocean to air, and now cyberspace, where we today see that it has become a new arena of conflict.

This paper explores how intelligence professionals can improve collaboration, integration, and analytical capabilities to identify national security risks, interests, and opportunities. Intelligence services provide strategic intelligence, provide in-depth assessments and developments to recognize and warn of changes related to specific issues that will affect the strategic environment in the future.

The strategic early warning community must have its overall impact measured by one criterion: the extent to which its assessments actually add informational and analytical value to the national decision-making process. This requires a qualitative, rather than a quantitative, judgment by policy elites. The strategic intelligence community must thus be granted the authority and autonomy to best carry out its responsibilities free from artificially- imposed impediments created by the clumsy application of unresponsive bureaucratic norms.

The policymaker may wish to know the weapons capabilities of adversaries and location of their warfighters. The amount of information that could be valuable in making political, economic, diplomatic or military decision making is potentially vast, and the collection is limited only by the resources available to a nation to fund networks of surveillance satellites, reconnaissance aircraft and listening devices.

2. Intelligence has changed

An intelligence product is successful when it informs the decision-maker, policy-maker or military leader with the necessary information and answers to win on their playing field. Intelligence analysis is a vital tool of modern security and many people may be unaware of the key role it plays. The aim of intelligence analysis is to conduct a detailed review of information collected in order to make informed decisions. Today, the threat landscape is changing. In an evolving world, understanding how criminals operate in increasingly complex ways is key to making informed decisions about security.

Early warning and early response will be faced with an evolution of threats over the next decade. These threats will come from the combined impacts on conflict and instability of climate change, fallout from ongoing wars, fallout from the war on terror, and the increasing criminalization of conflict. Indeed, the future relevance of the field depends largely on work undertaken now to understand and provide useful analysis on these new emerging threats.

The National Security Intelligence environment is undergoing profound changes. Powerful new technologies enable the collection, communication and analysis of national security data on an unprecedented scale and now have a central role in intelligence practice. The increasing use of algorithms in intelligence operations also raises a wide range of issues regarding the human-machine relationship in these operations, the ability to exploit such technology to disrupt elections and other political processes, and the stability of traditional analyst culture in the intelligence community. It is almost inevitable that in this context of prophecies of change, a debate about adaptability and the refrain of information systems in a variety of countries.

Two features are remarkable about these end-of-century reflections on intelligence. The first is that they often present pronounced expectations of change, despite the fact that intelligence services are commonly regarded as extremely conservative institutions, especially in authoritarian regimes. Moreover, these expectations are invested in a political institution that is itself a decrepit product of the 20th century and which has already been undergone a massive evolution since 1900.

The second aspect worth noting characteristic of these futurist thoughts is that they are frequently quite optimistic, in stark contrast to some of the apocalyptic pronouncements that have emerged in the wake of the gender war debates, economic degradation and ecological collapse. To some extent, imagining a future for the international intelligence community has become an exercise in tracking the paths and limits of political change itself.

Changing the way intelligence services operate is seen by many as a vital sign of health in the new post-Cold War security system international relations. The ability of intelligence services to radical changes in their traditional habits of secrecy, in the way they think about threats to national security, and to make decisions about priority targets for intelligence collection and analysis is also seen as a key a visible symbol of their government masters' willingness to adapt to the new realities and dangers of international politics in 21st century.

The fact that intelligence agencies will have to deal with issues such as international drug trafficking, environmental pollution, terrorism, illegal technology transfers, rapid environmental change and population movements is now accepted by intelligence professionals and public commentators alike. But how to assess the likely degree of change that will occur in the period ahead? Intelligence practice as one century gives way to the next? Two tools can help: knowledge of the historical evolution of intelligence services during the 20th century and, perhaps most importantly, a național perspective on the culture Bound determinate of intelligence agencies, and international perspective on the "*commonalities*" of intelligence. Such an international perspective can also serve to indicate the degree of convergence or divergence affecting national intelligence

communities in a global system, and can serve as a way of synthesizing evidence from historical surveys and comparative studies.

Strategic intelligence has two meanings: first, collection, analysis and dissemination of information about global conditions, especially potential threats to a nation's security; and second, based on this information, the use of secret intelligence agencies to help protect nation from harm and to promote its interests abroad. Strategic intelligence is, in essence, information and response, the link that a provides in the decision-making process is a critical one in the face of modem apocalyptic weapons and fragile economic dependencies.

Considerable effort has been put into defining the general term "*intelligence*", which certainly includes analysis as part of a multi-faceted process, obtaining specific, often secret, information for government use. Analysis is the thinking part of the intelligence process, or, as career analysts put it, "*Intelligence is a profession of knowledge*". It is about monitoring countries, trends and important people, events, and other phenomena in identifying patterns or anomalies in behavior and cause-and-effect relationships between key factors explaining past outcomes and which could point to future developments with policy implications for countries.

Another key founder of the CIA's analytical practices and principles put it this way more succinctly: *"The mission of intelligence analysts is to apply in depth substantive expertise, all-source intelligence, and a hard-nosed commercial operation to produce assessments that provide distinct value added to political clients*."(Regan, 2022).

"*Intelligence community*" is theoretically a generic term for the coordinated functioning of the national security system. Therefore, the intelligence community should not be confused with all the services specializing in protecting national security and safety, which are all the organizations with components in this field, but without a unified leadership and coordination, but rather disparate, depending on the duties of each institution.

It should be noted that the United States was the first to enact a law expressly providing for the definition of "*intelligence community*", and in Portugal, the role and functions of an Intelligence Community are carried out by the Intelligence System of the Portuguese Republic (S.I.R.P.), created by the Framework Law of the Intelligence System of the Portuguese Republic .

The fact that this system: contributes to covering the whole range of issues specific to the areas of national security; allows a unified approach to the managerial and functional problems of the intelligence structures that make it up; avoids parallelism and overlapping in the work of the intelligence services; allows a unified, efficient and qualified control, by areas, problems and profiles of activity, according to the competences and missions entrusted to it, gives the idea that this system was designed and represents a de facto "*intelligence community*" (Joseph, 2022).

Other democratic states have also set up structures involved in national security, which as a whole operate according to the principles of the "*intelligence community*". Adapting intelligence and security services to the new challenges of this millennium, creating new intelligence structures specialized by threat type, responding to the rapidly changing configuration of asymmetric threats, also requires the effective functioning of the National Intelligence Community, which can be an effective way of combating these threats.

The intelligence analyst plays a key role in enabling national security strategists to meet critical objectives. Although the analyst should not define a national security strategy, he must be aware of the what that national security strategy is, how the current set of decision makers define national interests and, therefore, the threats and opportunities to them, and the key policy objectives of those decision-makers. Currently, the analyst has the advantage, and challenge of understanding a long list of explicit security, homeland defense, counterterrorism, and intelligence strategies.

An analyst who has studied the strategic thinking of key policymakers is in a better better position to enable these strategists to improve their performance at every stage of the decision-making and policy execution process. Viewed in this context, virtually all intelligence analysis is

strategic because it aims to enable policy makers to achieve their objectives with the necessary means. Meaning, whether the analyst is describing the overall strategic environment or providing warning of a particular attack, simply describing the military details of an adversary potential or infrastructure of an adversary, or providing highly tactical information on targets, the analyst approach itself is in support of an overall strategy to achieve specific objectives, specific goals.

The intelligence service supports the cybersecurity of its own state by advising on and setting standards for defensive and protective security measures. It also provides intelligence threat assessments; engages in counterintelligence activities and seeks evidence of intelligence successes of hostile countries through counterintelligence penetrations of organizations and by examining the operational actions of these countries. The counterintelligence ('external intelligence') element of these activities is part of a specialized "*counterintelligence contest*" against adversaries.

All these activities support the intelligence services' own intelligence services security intelligence, as well as those of the government and its armed forces as a whole. Threats to the national security of intelligence services are now much less clear than in during the Cold War. But some defensive security will continue to be necessary because this will also require intelligence support, in particular the ability of the intelligence services to establish national defensive standards in the light of offensive experience. This is a factor to be taken into account in national decisions on the sophistication of collection required.

The importance of information on national security issues raises difficulties questions, such as how much knowledge (operational and non-operational) should be disclosed so as to inform the public concerned, without jeopardizing national security. Pursuing a fair and practicable balance between civil liberties and security is very difficult to realize and have occupied for a long time the minds of both practitioners and scholars alike. As in the most complex balancing dilemmas, there is no single plan adopted by all democracies to achieve this goal. National information laws, is the embodiments of different nationalities democratic will, have offered different ways to achieve such a balance. Regardless legitimate variety of such balancing efforts, all measures should be predetermined by principles of democratic governance. Among these principles is the doctrine of separation competences and the rule of law are relevant (Farson, 2021).

3. The Intelligence Community's fundamental role in the information war

An important difference between war and intelligence, is that in the case of the former there is a clear distinction between the right to go to war, *jus ad bellum*, and the justice of actions in war, *jus in bello*. This distinction does not work when thinking about cyber intelligence gathering. There is not the same division between the assessment and sanctioning of the general act of intelligence gathering and the carrying out of various acts under this authorization which is observed in the case of war. There is no *"wartime/peacetime*" distinction for Intelligence, but rather operations are conducted on a continuous basis. Thus, in the case of intelligence, the assessment must be made on a continuous basis, whereby each operation must meet all the right conditions cyber-intelligence principles described later, an operation being sanctioned depending on who is targeted, taking into account whether or not there is a specific cause for the operation, ensuring that there is a fair intent and that the method chosen is proportionate to the gains proposed (Hew, 2022, p. 7).

One of the main challenges for states in ensuring cybersecurity is the speed with which new threats and risks materialize, often one step ahead of legislation and institutional procedures designed to keep cyber threats at bay. In a nation like Romania, where legislation must be coordinated through the EU process, states can find themselves working particularly hard to keep up with new risks and challenges. At EU level, apart from the General Data Protection Regulation (which covers privacy of users and protection of personal data), the most important piece of cybersecurity legislation is the NIS Directive on network and information systems security, which is

a significant part of the EU's cyber security strategy. As a member of the EU since 2007, Romania is obliged to transpose all EU legislation at national level and to make appropriate amendments (Branda, 2021).

Cybersecurity is no exception in this respect, since, unlike the classic classical threats, which require already established defense mechanisms, cyber-related threats require constant adaptation of response mechanisms, as well as technological innovation, allocation large sums of money, and clear legislation to address the threat in question, and eventually neutralize it at source. Although cyber threats have been around since processes such as banking, transport, water, healthcare and industrial infrastructure have become heavily connected to the internet dependent, Romania's cybersecurity capability could easily be described as a long-term "*work in progress*". Thus, an investigation of Romania's cybersecurity efforts focuses on the following aspects: legislation and institutional framework, threats and countermeasures efforts these threats (Herman, 1997).

4. How the Intelligence Secret Services will change after the Russia-Ukraine War

Russian President Vladimir Putin's chosen war in Ukraine is a world historical event, marking the last act of the post-Cold War era and the beginning of a new, as yet unwritten era. The spectrum of possible outcomes ranges from a new or hot, volatile cold war involving the United States, Russia and China, to a frozen conflict in Ukraine, to a post - Putin agreement in which Russia becomes part of a revised European security architecture. With the West imposing unprecedented sanctions against Russia in record time and with the real potential of descending into nuclear war, we are in uncharted territory. It is hard to see how Putin could "*win*". But he cannot accept defeat.

To help policymakers imagine what might happen next and find ways to prevent a worst-case scenario, the following four scenarios have been developed on how this war might end and the future geopolitical alternatives that could result, transforming international relations over the next two to three years: a frozen conflict, a double cold war, a nuclear apocalypse and a brave new world.

When we talk about the international order, we sometimes refer to the balance of power between states and sometimes to the set of rules and norms that affect their relations. Putin's invasion did serious damage to the normative order, but the UN ban on the use of force to change borders has already been violated by the US in Kosovo in 2009 and by Russia in Crimea in 2014. Whether or not this important norm can be restored remains to be seen, but most ONU states have a strong interest in preserving their sovereignty.

After the 2008 financial crisis, Russia and China began to suggest that the US was in decline, but the US share of the world economy has remained surprisingly constant for decades. Even if the size of China's economy (as measured by exchange rates) overtakes the US in the next decade, and China tightens its alliance with Russia (which has an economy the size of Italy), the two together will not come close to matching the combined economic strength of the US, Europe and Japan.

The crisis in Ukraine has presented the United States with a complex set of challenges and opportunities. It has brought the transatlantic alliance together, even as it pushes European countries to build more independent capabilities of their own, which is a diplomatic victory for the Biden administration. However, the Russian invasion marks the definitive end of the US-led liberal international order that was founded after the Cold War (Friedman, 2022, p. 21).

The war in Ukraine will also help Beijing assess what the world's response would be to a Chinese invasion of Taiwan. The speed and fury with which the United States, Europe and the major Asian economies (Japan, South Korea, Singapore, Australia) imposed severe sanctions on Russia almost certainly came as a shock to China's leaders. The swift Western response will give ammunition to Chinese advocates of more complete decoupling of the country's financial system

from the West. Beijing's goals, as part of the Made in China 2025 initiative to become self-sufficient in key high-tech areas, and China Standards 2035, an effort to shape trade and technology standards and rules, seem even more urgent (Ses, 2019, p. 13).

China has a chance to play a much bigger role on the world stage if Xi can convince Putin to stop the war and agree to peace talks. At the moment, China is reluctant to do so. In the Brave New World scenario, however, the prospect of World War III convinces China to step in and bring Putin to his senses, laying the groundwork for a lasting peace agreement between the West and Russia.

The war is now being waged by mobile phones, social media and private surveillance satellites. Information has always been an important part of Soviet and Russian doctrine, but now access to information is more widely distributed and harder to control. It has always been true that success in war depends not only on the army that wins, but also on the story that wins. But in the information age, it is more difficult than ever to control the story. Not only did Biden's disclosure spoil Putin's planned narrative, but so did Ukrainian citizens record the war with their cell phones. It is far too early to predict the future of Putin's invasion. You can imagine a spectrum of futures regarding Ukraine, from a formal incorporation of Ukraine into Russia and a protracted Cold War, to the long-term undermining of Putin and a weakening of his alliance with China (Huw, 2022, p.3).

A strategy of great power competition between a democratic and an authoritarian bloc may help America mobilize support domestically, but it brings together very different types of states. Russia is a declining power and China a rising one. The US needs to appreciate the unique nature of the threat posed by Russia. Today, Russia is in demographic and economic decline. Its economy is dependent on oil and gas exports and has failed in its efforts to transform its economy, as the US and China have done. Russia retains huge resources, including mercenaries and proxies, which it can use as spoilers in cyber conflicts and in the Middle East and Africa. Now Putin has used these resources in his effort to "*make Russia great again*" by invading Ukraine. But if this cuts Russia off from European and American technology, history may judge Putin as a great tactician but a failure as a strategist who has achieved his goal of restoring Russia's place in the world.

When thinking about how the war in Ukraine will end, we must first understand how it began. Russia invaded for geostrategic reasons - having Ukraine as a buffer state protects Moscow from invasion from the West - and for economic reasons, which have often been overlooked. The transition from the Soviet Union to the Russian Federation was not exactly profitable. Total wealth may have increased, but Russia remains a poor country. Its gross domestic product ranks just behind that of South Korea, a respectable placement, but hardly where a superpower should be.

Today, the Russian military seems disorganized, unimaginative and uninspired. Force deployment, logistics preparation and battlefield command at all levels simply did not exist. This was a different kind of Russian army, a bureaucratized one, one that feared the Tsar more than losing to the enemy. Putin called for a swift defeat of the enemy. But to lead by force, you have to see clearly and strike decisively at the center of gravity.

Ukraine had no center of gravity, only a widely dispersed light infantry force that offered no single point of destruction. While this may appear to be guerrilla warfare, it is not, and Ukraine surprised its enemy with its resilience and unpredictability. The attacker may respond with brutal attacks on the population, but this leaves Ukrainians no choice but to fight. The Russian military was not designed for this war, did not plan for this war, and has only brutal countermeasures to take against civilians. And Putin will take it.

The problem, then, is that Putin can't stop, nor can he reach an agreement with Ukraine that he will respect. Any agreement, short of surrender by the enemy, is a revelation of weakness on the part of a weak country and a weak leader. The only alternatives are ineffective actions, because the force he sent to war was the wrong force in the wrong country.

The Russian invasion of Ukraine has brought about a major change in intelligence services, especially in America and Europe. In the process of modernizing intelligence, the priorities over the

next decade will be: better-defined defense imperatives, modernizing capabilities to counter new Russian and Chinese challenges, technologies that are difficult to detect and defeat. The United States has clear defense strategy priorities in this regard.

Intelligence has warned of Russia's intentions in Ukraine. Political factors have chosen to make public the warnings they have received. The same politicians have emphasized the accuracy of the reports since the invasion and praised their intelligence services. The UK Defense Intelligence Service posted daily on the social media accounts "*Information Updates*", assessing Russia's progress in its invasion. The war, and especially the presence of the war, placed the intelligence agencies in a very public position. Their product was used to inform the global public, to counter Russian misinformation and as part of a deterrent package. It will play a crucial role in the coming days and weeks, both in public and in secret.

The decision to use information in public is not without precedent. There is a long history of states declassifying documents or strategically leaking selected material to certain audiences for certain purposes. It didn't always go well. The ghost of "*slam dunk*" information about Iraq's weapons of mass destruction, infamous files and the ensuing painful revelation of a catastrophic failure is looming large in public and no doubt in the mind of the intelligence officer when he considers public information. The above controversies, however, should not blind us to the usefulness of using the state's intelligence power in public.

The use of public information in the run-up to this war was unprecedented in its scale. This has been helped, in part, by the relative ease with which modern intelligence powers (and indeed the average citizen with a limited budget and an Internet connection) can monitor the movement of aircraft, formations and armor in space, through the technique of open source (OSINT). The mass mobilization was visible, eloquent, revealed a clear capacity and indicated a hostile intention. Public disclosure denied Russia the advantage of the surprise and undermined its claim that it was a peacekeeping operation. Its use denied Russia the initiative in the information space.

The United States, consistent with its defense strategy, values and prioritizes the creation of an integrated deterrence structure and a first strike/response window of opportunity. This deterrence is integrated in that it considers five categories:

- All domains (conventional, nuclear, cyber, space, informational);
- All theatres of competition and potential conflict;
- All aspects of the conflict spectrum (from high intensity warfare to the grey area);
- All instruments of national power (economic sanctions, diplomatic instruments, etc.);
- All US allies and partners (Europe, Asia, Americas, etc.).

The US does not want to be in a vulnerable position, as it was during the Cold War. This fears falling behind the development of new Russian and Chinese technologies. These technologies, such as hypersonic vehicles, which Russia has been testing in the Arctic over the past year, can evade ground radars by hiding behind the Earth's curvature. Thanks to their speed and maneuverability to evade defenses, these missiles are extremely difficult to detect and defeat.

The United States is pursuing two key technologies to win this race: boost-glide systems that place a hypersonic glide vehicle on top of a ballistic missile booster, and hypersonic cruise missiles that would use "scramjet" technologies (allowing efficient operation at hypersonic and supersonic speeds). Hypersonic weapons will allow the US to be a credible deterrent against China and Russia, which already have functional hypersonic weapons.

Ukrainian war is a warning that we should be spending more on research and development that improves unmanned air systems, both in ground attack and in anti-air capacities; leverage improvements in artificial intelligence to make them operate synergistically together; and experiment with such capabilities aggressively to be able to provide close air support from higher altitudes and with unmanned, less expensive vehicles controlled directly by ground forces.

While intelligence gathering in the 21st century is likely to be dominated by intelligent machines, the value of intelligence will continue to reflect the acumen of the human mind. No amount of raw data can substitute for an insightful analyst able to discern critical policy or operational significance of an event, action or trend that might be hidden in a mass of confusing and contradictory information. In attempting to quantify the value of polished, high-quality intelligence, former US Secretary of Defense James Schlesinger remarked, "*when you have good analysis, on a scale of 1 to 10 it is more valuable than data*" (Burrows, 2022)

Intelligence Services will be forced to strengthen and diversify the scope of their collection and assessment activities in response to new security threats such as terrorism, cross-border organised crime, illegal immigration and environmental degradation. These non-traditional security threats have been placed on the international security agenda with increasing frequency over the last decade and are beginning to be reflected in national intelligence priorities (Burrows, 2022).

5. Intelligence Analysis early warning systems will improve in the future

Strategic warning intelligence must be able to provide early assessments of future problems to avoid strategic surprise. Senior leaders must be sufficiently well informed so that no single event, however catastrophic, can overwhelm them and paralyses their responses. This is an increasingly difficult task, and one that becomes more problematic as the complexity of the international environment increases.

Good strategic early warning information is also key to a number of non-traditional areas of concern, such as transport security, social resilience, supply chain management, criminal and health issues. Without advance knowledge, all these policy areas are subject to disruption and shock. What are the requirements for good strategic early warning in the future? Perhaps the most important requirement is to realise that intelligence is a very different function from the rest of government and must be allowed to operate as such. A weekly approach is not enough for strategic level analysts. Intelligence staff need to be deeply motivated and very dedicated to their work. The functions they perform in their work must closely reflect their education and personal interests. No application of methods and processes will be sufficient if the key personnel involved do not have the necessary training and interests.

Leveraging the strategic early warning analyst. In essence, if policy makers truly want to develop an effective strategic early warning capability, much more than seeking and relying on technological solutions, effective human resource development is crucial. This means hiring promising people and being prepared to develop and train them over a period of years. It takes five or seven years of initial training to produce a doctor or vet, plus a few years of experience after that. Arguably, given the increasingly complex security environment, the role of the strategic early warning analyst is at least as important as that of the veterinarian, so why not require the same level of training for this person?

Moreover, the career path of strategic intelligence analysts must be designed with the logic of continuity of trained and motivated expertise in mind. Endless rotations of analysts in and out of positions to ensure a "*seamless*" flow of personnel in accordance with an overall staffing plan too often leads to the creation of a short-term risk-averse mentality among officers, which can be detrimental to the effectiveness of the overall strategic analysis process. In addition, analysts need to feel confident that they can tell the truth without fear of negative consequences. Being an intelligence analyst means being able to bearer of bad news or presenting views that contradict the intentions and opinions of important and powerful people.

Anticipatory intelligence involves collecting and analyzing information to identify new, emerging trends, changing conditions, and underestimated developments that cast doubt on long-standing trends and assumptions and encourages new insights, identifies new opportunities, and

warns of threats to states' interests. Anticipatory intelligence typically harnesses an interdisciplinary approach and often uses specialised techniques to identify emerging problems from 'weak signals', cope with high degrees of uncertainty and consider alternative futures.

Anticipatory intelligence looks to the future as foresight (identifying emerging issues), forecasting (developing potential scenarios), or warning. It can uncover groups or regions that were previously unconnected and include indicators or benchmarks to identify key developments as trends change over time. Anticipatory intelligence assesses risks, information gaps and uncertainties by assessing the likelihood of occurrence and the potential effects of a particular development on a State's national security.

Finally, in today's complex and uncertain security environment, strategic early warning analysts do not have the luxury of tunnel vision. Analysts increasingly need to get out of government circles on a regular basis to talk to like-minded people in think tanks, industry, and other parts of government. It is not an aberration to say that most of the expertise and knowledge needed for effective strategic early warning analysis is now outside government. Therefore, extra-governmental expertise must be tapped and systematically engaged (Quiggin, 2006).

Warfare in the future is not going to be conducted by machines, no matter how far AI advances. Warfare will instead be connected human to human, human to internet, and internet to machine in complex, global networks. We cannot know today how such warfare will be conducted or what characteristics and capabilities of future forces will be necessary for victory.

In the decades to come, the forces of change will continue to play their part, reshaping and transforming the art/field of intelligence in a myriad of directions. As intelligence becomes more affluent and less privileged in the 21st century 'global information environment', paradoxically the demand for rapid, high quality strategic and operational intelligence will intensify rather than diminish. The ever-increasing volume of intelligence will be a test of a different kind for the analysts, warfighters and decision-makers of the future. Yet the essence of the intelligence dilemma will remain - how best to reduce the element of risk for decision-makers and illuminate what would otherwise be unknown?

Also, in the rush to reduce costs and reap more rewards from expensive intelligence assets, commercial and OSINT technologies will supplement, reinforce and sometimes replace the classified systems that dominated intelligence collection during the Cold War. but although classified material will be a smaller proportion of total user intelligence, it will provide critical pieces of the intelligence puzzle. Classified collection methods are generally more useful for current assessments and sensitive, hard-to-get military or technical information than for long-term forecasting and economic analysis.

Non-state actors will pose challenges of a different nature. Operating in the shadows, adept at the art of deception and disguise, terrorists and criminals may be more difficult to identify, locate and eliminate than political leaders or military forces of enemy states. Expensive, high-tech intelligence systems designed for conventional warfare or monitoring the electronic environment could be ineffective against these organizations that use simple clandestine communication methods, as Osama bin Laden demonstrated with the well-coordinated attack on the United States that has been labeled by some as the "Pearl Harbor" of this century. Despite impressive breakthroughs in sensors, automation, technical collection and decoding, it remains for humans to provide the cutting-edge intelligence. And it should be noted that there is no substitute for effective managers, precise analysts, capable linguists and dedicated agents.

The traditional intelligence cycle clearly has less explanatory and organizational utility in the post-Cold War world. The discrete functionality implied by separating intelligence processes into collection, collation, analysis, and dissemination reflects the concepts, practices, and organizational dynamics of an earlier era. What will distinguish the success of 21st century intelligence specialists will be the ability to fuse and integrate all elements of the process to provide different types of

support to decision makers and operational commanders. It is worth noting that the bureaucratic walls that once separated intelligence producers from intelligence users are coming down at a rapid pace, removing artificial and dysfunctional distinctions between strategic, operational and tactical intelligence assets. The imperatives of modern warfare, particularly IW, will reinforce the need for holistic intelligence and erode the distinction between operations and intelligence (Bijleveld, 2020).

6. Conclusions

Future intelligence operations will enable success in the cognitive domain. However, to achieve superiority in the cognitive domain requires an immediate rebalance of current investments to provide a totally new information foundation, refining or removing policy barriers to sharing of information, and providing a robust architecture to rapidly share that information. Providing for immediate and proactive deployment of that infrastructure requires a new means of communication and new varied sensors/capabilities to capture new information sets. Such activities will provide a sustained means to conduct and enable proactive influence operations and advance predictive analysis. Advancing proactive influence operations and predictive analysis to win in the cognitive domain requires new expertise, reviving old tradecraft, and advancing new levels of integration towards a whole of government/nation approach to national security.

The good news is that the means, technology and information to achieve such capabilities are readily available in today's commercial markets. The investments and capabilities realized in-turn provide an absolutely critical foundation to winning any kinetic conflict. This foundation also serves another critical purpose – achieving success in post conflict efforts towards ensuring sustained peace. Developing these capabilities, foundation and expertise requires a sustained national effort, now through 2035, in establishing the baseline capability that will upset the dynamics of our adversaries, causing them to react to our efforts. We need a broad and in-depth strategy for influence operations and predictive analysis. We are in a cognitive war, and it is a war of a millennia, not years, decades or centuries.

The unprecedented acceleration of change and the deepening of the gap between the former and the latter may threaten the fragile governance of institutions. Faced with this asymmetric and dynamic environment, intelligence professionals will have to assess the security environment marked by regional, economic, resource and ideological competition. This will require accelerated action to transform intelligence in several key directions:

- faster modification and adaptation of the legal framework - not post factum - to the reality of new security threats and risks.
- Exploring intelligence concepts, strategies, policies and technologies to meet the requirements of beneficiaries and concerted threats;
- Integrated Systems with Strategies .
- accelerating forms of interagency cooperation
- Streamlining intelligence work and agency/service capabilities provided through and by the Intelligence Community (IC) to meet the "changing" needs of security intelligence users. This will mean a planned approach to knowledge transfer, ensuring a continuity of formal and informal data sets, which will not be lost with the replacement of human resources (departure of some staff and arrival of others).
- creation of general ethical standards;
- increasing the amount of common training within the Intelligence Community
- formalising requirements for further training within the IC;
- Possibility for IC members to share information systematically creating a basis for identifying IC and non-governmental expertise;
- Mandating rotational themes for IC members;

- Institutionalisation of the development of new ideas;
- allowing IC members to leave and rejoin the IC without penalty;
- implementing common recruitment policies at IC level;
- the establishment of a common personnel system at IC level;
- formal mentoring programmes at IC level;
- hiring an adequate number of analysts to provide opportunities for career development, training and rotation;
- Achieving a full rotation outside the agency - mother to be a requirement for promotion;
- recruiting analysts with non-traditional backgrounds;
- developing a programme to identify and use non-governmental experts.
- Many of these goals are revolutionary. Others, though bold, are evolutionary.

These actions are necessary to prepare a strategic shift in the face of challenges that can be foreseen, and - just as importantly - to prepare those new strategies for new challenges that cannot yet be foreseen.

Of course, no intelligence system, no matter how effective, will be able to solve all the challenges in the security environment. What will mark the success of 21st century intelligence specialists will be the ability to merge and integrate all elements of the process to provide different types of support to decision-makers and operational commanders.

The future in Intelligence indicates that intelligence will move from being a key facilitator to being the leader of proactive influence operations in the competition phase. Regardless of who leads, cognitive operations will require a new construct that does not exist today. Such operations will require an integrated set of intergovernmental governmental intelligence, intelligence, cyber, policy, technology, and so on. Operations are likely to be further activated through back-to-back contact with an extensive network of sub-ecosystems providing expertise in economics, criminal, financial, commercial, cultural profiling, etc.

The new findings will increase the contribution of intelligence to national security, albeit with its own risks and shortcomings. Prudence and historical experience suggest, leaders and commanders will maintain a healthy degree of Clausewitzian skepticism about intelligence's ability to completely eliminate the difficulties and uncertainties involved in trying to divine the intentions and capabilities of others, especially in wartime.

By 2035, the defense organization will be more smart and technologically more advanced. He will have a great ability to adapt to situations and will and will act on the best information. Digital threats around the world will increase in the coming years and the gray area between war and peace will grow. The defense organization will be called in more and more frequently, and intelligence analysts will need to be trained, equipped and trained.

References:

[1]. Ank Bijleveld-Schouten, (2020). *Defence Vision 2035 Fighting for a safer future*, Ministry Of Defence.
[2]. Camille Raymond, (2022). *New Technologies, Climate Change and War in Ukraine: What Impacts on NORAD Modernization?* Policy Report, Network For Strategy Analysis. Queen's University, ras-nsa.ca.
[3]. Dupont Alan, (2003). *Intelligence for the Twenty First Century'*, lead article in special edition of Intelligence and National Security, vol.18, no.4, Winter, pp.15-39.
[4]. Edward L. Ses, (2019). *Future Military Intelligence CONOPS and S&T Investment Roadmap 2035-2050, The Cognitive War*, Haugland.
[5]. George Friedman, (2022). *How the Ukraine War Will Likely End*, Geopolitical Futures.
[6]. Huw Dylan, (2022*). How has public intelligence transformed the way this war has been reported?* Kings College London.

[7]. Joseph S. Nye, (2022). *Has Putin's invasion changed the world order?,* The Spectator.
[8]. Lahneman, William (2007). *Is a Revolution in Intelligence occuring?*, International Journal of Intelligence and Counterintelligence, pp.1-17.
[9]. Loch Johnson, (2007). *Handbook Of Intelligence Studies*, Routledge Taylor and Francis Group, London.
[10]. Maior George, (2008). *Noul aliat: regândirea politicii de apărare a României la începutul secolului XXI*, Editura Rao, Bucuresti.
[11]. Mathew Burrows, (2022). *How will the Russia-Ukraine war reshape the world?* The Big Story, Atlantic Council.
[12]. Michael Herman (1997). *Intelligence Power in Peace and War*, Royal Institute of International Affairs.
[13]. Mitt Regan, (2022). *National Security Intelligence and Ethics,* Studies in Intelligence, Routledge, Taylor and Francis Group, London.
[14]. Oana-Elena Brânda, (2021). *Romanian cybersecurity efforts: a work in progress,* Routledge Companion to Global Cyber Security Strategy, New York.
[15]. Roger George, (2008). *Analyzing Intelligence – Origins, Obstacles and innovations*, Center for Peace and Security Studies, Edmund A. Walsh School of Foreign Service Georgetown University.
[16]. Stuart Farson, (2021). *Security and Intelligence in Changing World,* New perspectives for 1990s, Routledge, Taylor and Francis Group, New York.
[17]. Tom Quiggin, (2006). *The Future of Strategic Early Warning*, Rajaratnam School Of International Studies, Singapore.
[18]. Tănase Tiberiu, (2010). *Cooperarea în domeniul intelligence-ului în spațiul european şi euroatlantic*, Universitatea Naţională de Apărare, Editura UNAP.
[19]. Tănase Tiberiu, (2010). *Consideraţii privind impactul ameninţărilor globale asupra comunităților de Intelligence. Importanţa modelării acestora prin noi strategii de securitate şi întelligence*, Editura ANI București.
[20]. Tănase Tiberiu, (2010). *Puncte de vedere privind departamentul şi strategiile privind securitatea şi Intelligence-ul patriei*, Editura Universitătii Lucian Blaga, Sibiu.
[21]. Tănase Tiberiu, (2009). *Transformarea intelligence-lui în contextul noilor provocări ale secolului al XXI-lea*, Revista Română de Intelligence Nr. 1-2.
[22]. Tănase Tiberiu, (2010). *Intelligence-ul Apărării din SUA - comunitatea şi strategia de Intelligence din Departamentul Apărării*, Gândirea Militară Românească nr. 2.