EXPERIENCE OF US INTELLIGENCE SERVICES IN ASSESSING NATIONAL SECURITY THREATS TO IMPROVE THE EFFICIENCY OF THE NATIONAL THREAT AND RISK ASSESSMENT SYSTEM OF UKRAINE

Andrii Stroiev

PhD student, e-mail: andriyvolf683@gmail.com

Ministry of Defense of Ukraine, Kyiv, Ukraine

Received: June 10, 2025 | Revised: June 19, 2025 | Accepted: June 30, 2025

DOI: https://doi.org/10.33445/psssj.2025.6.2.5

Abstract

This article examines the experience of US intelligence services in the field of assessing national security threats and the possibility of its use in Ukraine. The place and role of US intelligence agencies in the system of detection and analysis of current threats are determined. It is clarified that in modern conditions, given Russia's armed aggression against Ukraine, the implementation of the best world approaches to threat assessment is extremely relevant. The normative documents, strategic approaches, and practical measures applied by the US intelligence community for the identification of dangers and assessment of national security risks are analyzed. Directions for the implementation of American experience to improve the efficiency of the national system of threat and risk assessment in Ukraine are proposed.

Key words: national security, threats, risk assessment, intelligence, special services, USA, experience, national resilience.

Introduction

An effective threat assessment system is a key factor in ensuring the national security of the state. The evolution of approaches to identification and analysis of security threats demonstrates that earlier efforts were focused on developing security strategies and concepts that recorded a list of current dangers. This state of affairs was explained by both objective and subjective factors, in particular, the periodic change of the geopolitical situation and the priorities of states' security policy. As a result, over the past decades, there has been a reassessment of threats and a revision of strategic documents in the USA, NATO, and European countries in order to take into account new challenges (terrorism after 2001, aggressive actions of the Russian Federation after 2014, cyber and information attacks, etc.). For example, the National Security Strategy of the Republic of Poland of 2020 comprehensively reflects the security environment, lists military, economic, energy, social, and climatic threats, and defines appropriate measures of state policy.

Today's security situation is characterized by the emergence of qualitatively new threats, which necessitates improving approaches to their assessment. As US President Joe Biden has repeatedly noted, the world has entered a period of acute strategic rivalry, comparable in scale to the beginning of the Cold War or the period after the September 11 attacks. The strengthening of China and the revanchism of Russia create serious geopolitical challenges, existential threats are growing (climate change, pandemics, etc.). At the same time, the technological revolution (microchips, artificial intelligence, quantum computing) is changing the nature of confrontation, providing opponents with new tools for conducting hybrid warfare. In such conditions, for effective counteraction to dangers, states must quickly adapt their national security and intelligence systems.

This is especially relevant for Ukraine, which, as a result of the military aggression of the Russian Federation, faces an unprecedented range of threats. Therefore, the relevance of the topic is determined by the need to implement the principles of proactive assessment of threats and risks, developed by leading special services of the world, as well as awareness of the urgency of strengthening the national system of early detection of dangers.

Research question

The problem of identifying and assessing national security threats has been considered in the works of both domestic and foreign researchers. The Strategy of National Security of Ukraine of 2015 and the Law of Ukraine "On National Security" of 2018 defined the basic terminology and general approaches to the formation of the national security system, including a list of the main threats. At the same time, experts noted the shortcomings of the previous regulatory approach – in particular, the fixation in legislation of a static list of threats, which does not correspond to the practice of NATO/EU and complicates timely response to changes in the situation. Certain aspects of countering threats are studied in the works of Ukrainian scientists: V. Lipkan analyzed the concept of the system of ensuring national security of Ukraine and the structure of security entities; O. Kuropyatnyk considered the nuclear factor in the confrontation between the USA and Russia in the context of the war in Ukraine; O. Novikova and O. Pankova compared the strategic security priorities of Ukraine and Poland. The Strategic Concept of NATO 2010 p. (Strategic Concept for the Defence and Security of the Members of NATO, 2010) and the new National Security Strategy of Poland 2020 p. (Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej) emphasized the change in the nature of threats and the importance of resilience in the face of hybrid challenges. Some publications of the National Institute for Strategic Studies highlight the issue of risk assessment: in particular, an analytical report by O. Reznikova et al. (2020) summarizes the best world practices of national risk and threat assessment systems and proposes new opportunities for Ukraine (Reznikova, O.O., Voitovskyi, K.Ye., & Lepikhov, A.V., 2020). An important source is also the White Book of the Foreign Intelligence Service of Ukraine (2021), which contains an assessment of current external threats to the security of Ukraine and emphasizes the need to implement the experience of leading special services of the world in domestic intelligence activities.

An analysis of scientific sources shows that although many works have been devoted to the problems of national security and strategic planning (Abramov, V.I., Sytnyk, H.P., Smolianiuk, V.F., et al., 2016; Horbulin, V.P., & Kachynskyi, A.B., 2010), the issue of forming a holistic system of threat assessment remains unresolved. In particular, there are no comprehensive studies that would detail the practical experience of US intelligence services in assessing threats and the possibilities of its application for reforming the Ukrainian security system. Only in some publications, they need to adopt the best intelligence practices of the USA (Burns, V. Dzh., 2024; Reznikova, O.O., Voitovskyi, K.Ye., & Lepikhov, A.V., 2020) is mentioned indirectly. Thus, the unresolved part of the general problem, which this article is called upon to answer, is the consideration of the experience of the American intelligence community in building an effective national system of threat assessment in Ukraine.

The purpose of the article is to determine the place and role of the experience of the US intelligence services in the process of assessing national security threats, as well as to substantiate the expediency and ways of using this experience in the formation of a modern national security system of Ukraine. In accordance with the goal set in the article, the following tasks are solved: 1) to analyze the approaches, mechanisms and instruments used by US intelligence agencies to identify and assess threats; 2) to outline the practical results of the implementation of American experience in threat assessment (on the examples of the activities of the US intelligence community); 3) to offer

recommendations for the adaptation of US experience in domestic practice of ensuring national security.

Results and Discussion

Practice of threat assessment in the US national security system. The United States of America has a wide-ranging intelligence community (the so-called Intelligence Community, IC), which includes 18 departments and organizations responsible for collecting and analyzing information about threats to national security. The activities of the intelligence community are coordinated by the Director of National Intelligence (DNI), a position that was introduced in 2004 as part of reforms after the September 11 attacks. One of the key tasks of the DNI is to combine data from all special services and prepare integrated threat assessments for the country's leadership. Starting in 2006, the DNI office annually presents to the US Congress the National Threat Assessment (Annual Threat Assessment) – a declassified report that contains an overview of the most important risks and threats to the United States for the current period. In this high-level document, American intelligence reflects its assessment of priority threats – from enemy states and terrorist organizations to cyber-attacks, the spread of weapons of mass destruction, transnational crime, and, more recently, global challenges such as pandemics and climate change. Thus, the United States has introduced a regular mechanism for strategic monitoring of threats, which allows timely informing legislators and the public about the dynamics of the security environment and developing sound policy solutions.

An important feature of the American approach is the combination of long-term strategic analysis of threats with an operational response to current risks. In addition to annual assessments, National Intelligence Estimates are prepared in the US on key security issues, as well as quarterly and situational reports for senior management. Intelligence agencies use advanced methodologies of analysis, including structured analytical methods, scenario modeling, "red teaming" methods, etc., to reduce the likelihood of miscalculations and ensure comprehensive assessments. To determine intelligence priorities, the National Intelligence Program and the National Intelligence Priorities Framework are used, which are regularly updated to reflect changes in threats. Thus, the American system is built on a flexible response – threats are not fixed once and for all in regulatory acts but are constantly monitored and reviewed in the course of interagency cooperation.

Particular attention is paid by the United States to the creation of institutional mechanisms for integrated threat assessment. Along with the DNI office, an important role is played by interagency centers and structures, such as the National Counterterrorism Center (NCTC), the Cyber Threat Center, the Cyber Threat Intelligence Integration Center (CTIIC), and others. They are designed to combine data from various departments in specific areas and produce a unified assessment of threats in the relevant field. For example, the NCTC, established in 2004, provides a joint analysis of terrorist threats, combining the efforts of the CIA, FBI, NSA, and other agencies. Similarly, cyber security integration centers collect information about cyber-attacks and intelligence in the digital space to prevent large-scale cyber aggressions. The presence of such coordination structures is an important element of the US experience, which has proven its effectiveness in preventing terrorist attacks and cyber-attacks.

In addition to purely intelligence assessments, the "all-hazards" approach operates in the US, which covers the assessment of all types of dangers - both hostile actions and natural disasters or man-made disasters. In particular, the Department of Homeland Security (DHS), together with the Federal Emergency Management Agency (FEMA), has implemented the THIRA (Threat and Hazard Identification and Risk Assessment) methodology for systematically identifying threats and hazards and assessing risks at the national and local levels. The THIRA process is carried out according to a standardized methodology and includes the identification of a list of the most

complex threats, the assessment of their impact, and the available capacities for response. For example, as part of the national THIRA 2019 assessment, 59 possible threats and hazards were analyzed, targets were set for the necessary state capacities to respond to the worst-case scenarios, and gaps that need to be addressed were identified. THIRA results are used to plan emergency preparedness and resource allocation, i.e., they actually integrate threat assessment into the national security management process. This practice is interesting for Ukraine because it allows involving a wide range of actors in the assessment of threats – from federal agencies to local communities and the private sector – and obtaining a coordinated picture of national risks.

Thus, the US experience in the field of national security threat assessment can be summarized in several key points. First, this is institutional development and coordination: the presence of a central coordination body (DNI) and specialized interagency centers that ensure the exchange of information and joint analysis. Secondly, regularity and systematic assessment: the production of annual and periodic threat reports covering the entire range of challenges, with constant data updates. Third, methodological diversity and a scientific approach: the use of advanced analytical methods (including the use of large amounts of open data, the use of artificial intelligence for information processing), which increases the validity of forecasts. Fourth, proactivity and flexibility: American intelligence tries not only to respond to existing threats, but also to predict their appearance, carries out strategic warning. A vivid example is the introduction of the practice of "strategic declassification" – the targeted public disclosure of certain intelligence data to undermine the plans of the enemy and mobilize allies. This step, applied on the eve of a full-scale invasion of the Russian Federation in Ukraine in 2022, demonstrated the innovativeness of the thinking of the US intelligence community. Fifth, the complexity of the approach: threat assessment is considered an integral part of the formation of national security and defense policy. Intelligence reports directly influence the development of strategic documents (such as the National Security Strategy, the National Defense Strategy, etc.), which ensures the unity of threat analysis and practical actions of the state. The new US National Security Strategy of 2022, for example, emphasizes the concept of "integrated deterrence" and the need for interagency coordination to counter the entire spectrum of threats – from military to economic and climate.

Significance of US Experience for Ukraine and Recommendations for Implementation. Given the current challenges facing Ukraine, the experience of American special services in assessing threats is extremely valuable. First, Ukraine should develop an integrated threat analysis system based on the US model. This involves creating a permanent interagency body (or improving existing structures of the National Security and Defense Council of Ukraine) to coordinate the activities of all intelligence entities for the detection and assessment of threats. In this context, it is useful to take into account the DNI model, which ensures the synthesis of information from military intelligence, external and internal (counterintelligence) intelligence in a single analytical center. Steps have already been taken in this direction in Ukrainian legislation: the Law "On Intelligence" (2020) has been adopted and a system of situational centers is being created under the National Security and Defense Council. However, it is necessary to move further – to the formation of a full-fledged national system of risk and threat assessment, which would function on a permanent basis, include all key departments of the security and defense sector, and also use the capabilities of scientific institutions and the expert community.

Secondly, it is worth introducing the regular practice of public reports on threats, following the example of the DNI's Annual Threat Assessment. There is already a positive precedent in Ukraine – the White Paper of the Foreign Intelligence Service, which presents an assessment of external threats and challenges to the security of the state. It is advisable to institutionalize such a practice and expand it: to prepare an agreed National Report (report) on threats to national security with open and closed parts, to present it annually to the parliament and the public. This will increase the

transparency of the security sector, public trust and the quality of public administration, because decisions will be made on the basis of clear analytical assessments.

Thirdly, Ukraine should adopt US methodological approaches to risk assessment, adapting them to its own conditions. In particular, it is worth testing the THIRA methodology at the national level: to identify a list of probable threats (military, terrorist, cyber, natural and man-made), to assess their potential consequences for the country and the state's ability to counter each threat. Such a comprehensive review would allow identifying the most critical gaps in preparedness (for example, insufficient air defense against missile threats, vulnerability of the energy system, lack of cyber specialists, etc.) and would contribute to prioritizing resources for their elimination. In addition, the application of the methodology at the level of regions and communities (with the support of the State Emergency Service and other services) would increase the overall resilience of the country to emergencies.

Fourth, it is necessary to invest in the development of the analytical potential of the intelligence agencies of Ukraine. US experience shows that the quality of threat assessment depends on the professionalism of analysts and access to modern data processing technologies. Therefore, it is advisable to introduce into the training programs for security sector specialists the best Western practices of intelligence analysis, to develop specialized courses (on intelligence analysis, forecasting, work with big data, etc.). In parallel – to equip analytical units with software products for data analysis, artificial intelligence systems, platforms for information exchange between departments. As CIA Director V. Burns notes, for the successful work of intelligence in the XXI century. It is necessary to combine traditional skills with new technologies, in particular, to provide analysts with tools based on artificial intelligence for processing colossal amounts of open and secret information. Ukrainian special services should adopt this approach, especially since the amount of intelligence data in modern warfare (satellite images, interceptions, OSINT, etc.) is extremely large.

Fifth, it is critically important to strengthen international intelligence cooperation and information sharing. The United States actively practices "intelligence diplomacy", that is, the interaction of intelligence services with allies for a common understanding of threats. Ukraine is already experiencing the benefits of such cooperation in the form of the exchange of intelligence data with partners in NATO in the course of countering Russian aggression. It is advisable to develop this cooperation further, to participate in joint projects on threat assessment (for example, regional security reviews of the Black Sea region, cyber exercises, anti-terrorism data centers, etc.). This will allow not only to obtain current information, but also to adopt methods and standards of threat assessment adopted in NATO countries.

In general, the implementation of US experience will require complex changes in the national security system – from normative-legal improvement (consolidation of strategic threat assessment procedures in doctrinal documents) to organizational reform of intelligence structures and training of personnel. However, such changes are necessary, given the unprecedented challenges facing Ukraine. As noted in the analytical report of the NISS (2020), the integration of the best world practices of risk assessment opens up new opportunities for enhancing the national security of Ukraine. Therefore, the experience of the US intelligence services should become one of the cornerstones in building a modern effective system of threat assessment and early warning in our state.

Conclusions

Based on the analysis, a number of conclusions can be drawn. First, the experience of the US special services in assessing national security threats demonstrates the high efficiency of an integrated, proactive, and scientifically sound approach to identifying dangers. The US intelligence community has developed a holistic system of strategic threat assessment, which includes regular analytical

products (annual assessments, thematic reports), interagency coordination, and the use of modern data analysis technologies. Secondly, for Ukraine, which is resisting military aggression and hybrid threats from the Russian Federation, the implementation of this experience is a necessary and important component of strengthening national security. The formation of an effective system of threat and risk assessment is one of the priority directions for increasing the defense capability and resilience of the state. Thirdly, the adaptation of the American experience should take into account domestic realities: political will and interagency cooperation are needed to create a unified platform for threat analysis, to improve the legislative framework, to develop the personnel potential of intelligence and to establish closer cooperation with partners. The implementation of these steps will ensure Ukraine's ability to respond in a timely and adequate manner to the entire spectrum of modern challenges, prevent crises, and effectively neutralize threats to national security.

Prospects for Further Research. Prospects for further intelligence in this direction include a deeper study of the practical aspects of implementing Western methods of threat assessment in the activities of Ukrainian special services. In particular, the issue of adapting the THIRA methodology and other risk assessment approaches to the national regulatory framework and the structure of the security sector needs to be studied. An interesting direction is also the analysis of the experience of other states (for example, members of NATO, Israel) in building early threat detection systems – in order to identify universal solutions and potential challenges in their implementation in Ukraine. Further research may be aimed at developing practical recommendations for creating an interagency center for threat assessment in Ukraine, developing a national system of indicators and markers of dangers, as well as integrating intelligence and analytical tools with partners for collective security. All these areas will be important for increasing the preparedness and resilience of Ukraine in the face of dynamic security challenges.

Funding

This study received no specific financial support.

Competing interests

The author declares that she has no competing interests.

References

Abramov, V.I., Sytnyk, H.P., Smolianiuk, V.F., et al. (2016). *Hlobalna ta natsionalna bezpeka* [Global and national security] / Edited by H.P. Sytnyk. Kyiv, NADU. 784 p.

Aleksandrov, O. (2015). Nova Stratehiia natsionalnoi bezpeky Polshchi – vidpovid na yevropeiski vyklyky ta zahrozy сьогодення [New National Security Strategy of Poland – a response to European challenges and threats of today]. *Stratehichni priorytety*, 1(34), 131–138.

Bila knyha. Sluzhba zovnishnoi rozvidky Ukrainy [White Paper. Foreign Intelligence Service of Ukraine]. (2021). Kyiv, SZRU. 72 p. Available at: https://szru.gov.ua/download/white-book/WB-2021.pdf.

Burns, V. Dzh. (2024). Shpyhunstvo ta derzhavne upravlinnia: transformatsiia TsRU v epokhu konkurentsii [Espionage and Public Administration: The Transformation of the CIA in an Era of Competition]. National Institute for Strategic Studies, 27.02.2024. Available at: https://niss.gov.ua/news/statti/shpyhunstvo-ta-derzhavne-upravlinnya-transformatsiya-tsru-v-epokhu-konkurentsiyi.

Horbulin, V.P., & Kachynskyi, A.B. (2010). *Stratehichne planuvannia: vyrishennia problem natsionalnoi bezpeky* [Strategic planning: solving national security problems]. Kyiv, NISS. 288 p.

Kachynskyi, A.B. (2013). *Indykatory natsionalnoi bezpeky: vyznachennia ta zastosuvannia yikh hranychnykh znachen* [Indicators of national security: definition and application of their limit values]: monograph. Kyiv, NISS. 232 p.

Kolodii, A. (2004). Natsionalna yednist i patriotism yak chynnyky natsionalnoi bezpeky [National unity and patriotism as factors of national security]. *Natsionalna bezpeka Ukrainy: Zbirnyk materialiv konferentsii ukrainskykh vypusknykiv prohram naukovoho stazhuvannia u SShA*, 25–30.

Kormych, L.I. (2021). *Harantii natsionalnoi bezpeky Ukrainy v yevropeiskomu konteksti* [Guarantees of national security of Ukraine in the European context]. National Institute for Strategic Studies. Available at: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosyny/garantiyi-nacionalnoi-bezpeki-ukrainy-v-ievropejskomu-konteksti.

Kuropiatnyk, O. (2015). Eskalatsiia yadernoho protystoiannia SShA ta Rosii u konteksti rosiisko-ukrainskoi viiny: dopovid [Escalation of nuclear confrontation between the USA and Russia in the context of the Russian-Ukrainian war: report]. Kyiv, Maidan of Foreign Affairs, June 2015. 41 p.

On Intelligence: Law of Ukraine of 17.09.2020 No. 912-IX. *Vidomosti Verkhovnoi Rady*, 5 (2021).

On National Security of Ukraine: Law of Ukraine of 21.06.2018 No. 2469-VIII (as amended by Law No. 2849-IX of 13.12.2022). Available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

Lipkan, V.A. (2003). Poniattya systemy zabezpechennia natsionalnoi bezpeky Ukrainy [The concept of the national security system of Ukraine]. *Pravo i Bezpeka*, 2(4), 84–89. Available at: http://nbuv.gov.ua/UJRN/Pib_2003_2_4_14.

Mizhnarodni vidnosyny ta polityka Ukrainy [International relations and politics of Ukraine] (collection of materials of NUOU named after I. Chernyakhovsky). (2020). Kyiv. 256 p.

National Security Strategy of Ukraine, approved by Decree of the President of Ukraine No. 287/2015 of May 26, 2015. Available at: https://www.president.gov.ua/documents/2872015-19070.

Natsionalna systema identyfikatsii zahroz i nebezpek ta otsinky ryzykiv (THIRA): ohliad ta metodolohiia [National Threat and Hazard Identification and Risk Assessment (THIRA): overview and methodology]. NISS, 25.07.2019. Available at: https://cip.gov.ua/services/cm/api/attachment/download?id=60358 (pdf).

Novikova, O., & Pankova, O. (2021). Osoblyvosti formuvannia ta realizatsii stratehichnykh priorytetiv zabezpechennia bezpeky ta rozvytku Ukrainy i Respubliky Polshcha [Features of the Formation and Implementation of Strategic Priorities for Ensuring the Security and Development of Ukraine and the Republic of Poland]. *Ekonomika – Upravlinnia – Innovatsii*, 2, 127–136. Available at: https://dspace.uni.lodz.pl/xmlui/handle/11089/41922.

Reznikova, O.O. (2013). Mizhnarodne bezpekove seredovyshche: vyklyky i zahrozy natsionalnii bezpetsi Ukrainy [International Security Environment: Challenges and Threats to National Security of Ukraine]. Kyiv, NUOU. 56 p.

Reznikova, O.O. (2018). Zabezpechennia natsionalnoi bezpeky i natsionalnoi stiikosti: spilni rysy i vidminnosti [Ensuring national security and national resilience: common features and differences]. *Visnyk Lvivskoho universytetu. Seriia filosofsko-politolohichni studii*, 19, 170–175.

Reznikova, O.O. (2022). *Stratehichnyi analiz bezpekovoho seredovyshcha Ukrainy* [Strategic analysis of the security environment of Ukraine]. National Institute for Strategic Studies, 14.01.2022. Available at: https://niss.gov.ua/news/statti/stratehichnyy-analiz-bezpekovoho-seredovyshcha-ukrayiny.

Reznikova, O.O., Voitovskyi, K.Ye., & Lepikhov, A.V. (2020). *Natsionalni systemy otsiniuvannia ryzykiv i zahroz: krashchi svitovi praktyky, novi mozhlyvosti dlia Ukrainy: analitychna*

dopovid [National systems for assessing risks and threats: best world practices, new opportunities for Ukraine: analytical report]. Kyiv, NISS. 84 p.

Stan ta perspektyvy stratehichnoho partnerstva Polshchi ta Ukrainy: analitychna dopovid [State and prospects of the strategic partnership between Poland and Ukraine: analytical report] (№ MEiN/2021). (2021). Warsaw–Kyiv. 112 p.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej [National Security Strategy of the Republic of Poland] of May 12, 2020 / President of Poland A. Duda. Warsaw, 2020. Available at: http://www.bbn.gov.pl/ftp/SBN%20RP.pdf.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej [National Security Strategy of the Republic of Poland]. (2014). Warszawa, Biuro Bezpieczeństwa Narodowego. 135 p. Available at: http://www.bbn.gov.pl/ftp/SBN%20RP.pdf (in Polish).

Strategic Concept for the Defence and Security of the Members of NATO. (2010). Available at: http://www.nato.int/cps/uk/natohq/topics_56626.htm.

Strategy of Development of the National Security System of the Republic of Poland – 2022. (2022). Warsaw: National Security Bureau. 48 p.

U.S. National Security Strategy and Defense Strategy of October 27, 2022. Available at: https://apps.dtic.mil/sti/trecms/pdf/AD1183514 (accessed: 12.06.2025).

Vorona, O.I. (2019). Systema analizu ryzykiv u sferi natsionalnoi bezpeky: teoriia i praktyka [Risk analysis system in the field of national security: theory and practice]. Kyiv, NISS. 92 p.

Yatsiuk, P.F. (2021). *Systema otsiniuvannia zahroz natsionalnii bezpetsi* [System for assessing threats to national security]: materials of a scientific seminar. Kyiv, NUOU.