Strategos, 9(1), 2025, 11-32
UDK 32
UDK 355/359
Review scientific paper

STRATEGOS

Examining the Transformation of the US National Security System after 2001

Ivana Pokrajčić[1]

Abstract

Today's security challenges are far more complex than ever before. The hypothesis of this article is that timely adaptation and innovation in response to new security circumstances, along with the development of innovative capabilities, are critical factors for effectively addressing the intelligence and defense challenges of the 21st century. Using a scientific approach through the analysis of available scientific research, congressional reports, and other relevant information associated with the United States of America (US) after September 11, 2001 (09/11), this article systematically explores the approaches taken by the US during the reformation of its national security system. It also synthesizes conclusions and identifies key shortcomings related to US national security system operations. The resulting conclusions and proposals in support of the stated hypothesis indicate that the transformation of national security related intelligence and defense systems require optimal reor ganization, the development of new and improved business processes, and the implementation of innovative technology that enable better and more efficient operation of the entire system.

Keywords:

contemporary security challenges, security system reform, defense system reform, security intelligence system, national security adaptation

1 Ivana Pokrajčić, Ministry of Defense of the Republic of Croatia, ivpokrajcic@gmail.com

INTRODUCTION

Three words describe the events in America since September 11, 2001:
Failure...reform...failure of reform.

Phillip H.J. Davies, 09/11
Final Report of the National Commission

The attack on the World Trade Center (WTC) was a global "security turning point", and September 11, 2001 was "the day that changed the world" (Davies 2012: 349). Pundits regularly draw parallels between the failure of the American intelligence community to anticipate Pearl Harbor and the WTC attack. Subsequent analyses of both events revealed that intelligence analysts and agencies ignored numerous indicators and warnings that the imminent attack on American soil would occur, and that there was a large terrorist supporting machinery behind the planned attack which was also located on American soil (Burch, 2008). In its efforts to support the hypothesis that timely adaptation and innovation in response to new security circumstances, along with the development of innovative capabilities, are critical factors for effectively addressing the intelligence and defense challenges of the 21st century, this article examines the transformation of US National Security System following 09/11. The hypothesis suggests that the ability to adapt quickly and innovate is essential to overcome the complex and evolving security threats in today's global landscape. It implies that failure to do so could lead to ineffective responses to modern intelligence and defense challenges. The scientific approach is based on structured, evidence-based methodology to analyze, compare and evaluate available scientific research related to US national security, including academic journals, studies, and theoretical frameworks relevant to intelligence, defense, and national security post-09/11. A significant part of the methodology involves reviewing congressional reports. These documents, such as those produced by the US Senate and House Intelligence Committees, offer insights into governmental inquiries and assessments of the national security system after 09/11.

The national security reforms following 09/11, at all levels, were immense. These included radical changes at the political level, the entire organizational

transformation of the security-intelligence system, and the creation of new tasks for the US Armed Forces. In the past 20 years or so, American federal level experts and the international scientific community investigated all aspects of the US national security system's reformation, its advantages and disadvantages, and the reformation's effects. Authors such as Burch, Davies, Sullivan, Massa, Klippstein and others based their theoretical research on detailed analyses of primary source data - congressional reports and independently conducted scientific research that provided an additional scientific contribution to the article's conclusions.

According to Burch, the US intelligence community's peacetime structure emerged from the creation of the Defense Department in 1947. These changes included organizational mechanisms such as new protocols for sharing information, and the process of directing and overseeing the work of intelligence services. This was the last major reformation until the conclusion of the Cold War (Burch, 2008). During the Cold War, intelligence committee analyses revealed deficiencies in analytical capabilities, duplicated efforts, excessive classification, and poor inter-agency intelligence sharing.

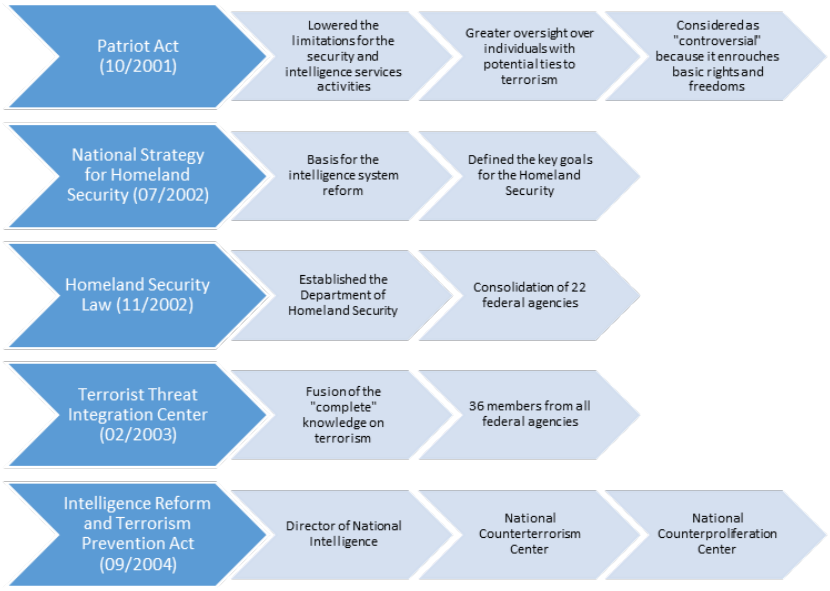
The WTC attack showed that the entire US security-intelligence architecture was overly restricted by bureaucracy and politics, and that "loyalty" to one's own agency took precedence over collective cooperation. Also, the analyses showed that the intelligence products of each of the intelligence agencies was under the influence of its "own corporate objectivity", which was potentially limited due to internal organizational factors such as biases, conflicts of interest, leadership, or even politics. After the 09/11 attack, theorists wrote for years about possible reasons for the US intelligence community's failure.

In examining why the failure occurred, the key question was: Could America, long viewed as an unequalled economic and security power, recognize and accept a real threat to itself? The second question was, if America was realistic enough to perceive and accept the possibility of such a threat, did the parochial and compartmentalized climate within the security-defense system contribute to the WTC failure? (Davies, 2012: 351). To answer these questions, Congress created two intelligence committees. Each encountered resistance during their investigations, both from the agencies themselves, which tried to conceal their failures, and from the George W. Bush administration itself,

which did not like to focus on its own failures. Without waiting for the final report, the Bush administration rapidly implemented corrective measures to improve the US's entire intelligence and defense systems. It wanted to give the Intelligence Community (IC) the capabilities the US desperately needed to detect and prevent future terrorist attacks on the country in a timely and effective manner (Sullivan and Lester, 2022:83).

The creation of the Homeland Security System after 2001 produced major organizational changes as well. Still, it did not replace or fully merge with the traditional national defense system led by the Department of Defense (DoD). Instead, these two areas became more interconnected while maintaining distinct roles. The Homeland Security Act of 2002 was signed into law by President George W. Bush on November 25, 2002. The Department of Homeland Security (DHS) was formally established on March 1, 2003, when it became operational by consolidating 22 federal agencies. The move represented the largest reorganization of the federal government since the National Security Act of 1947 with the creation of the DoD. These changes addressed all the identified shortcomings that contributed to the 09/11 attack and the IC's inability to predict and prevent the terrorist attack on the WTC.

Figure 1: The organisational and legislative changes post 09/11



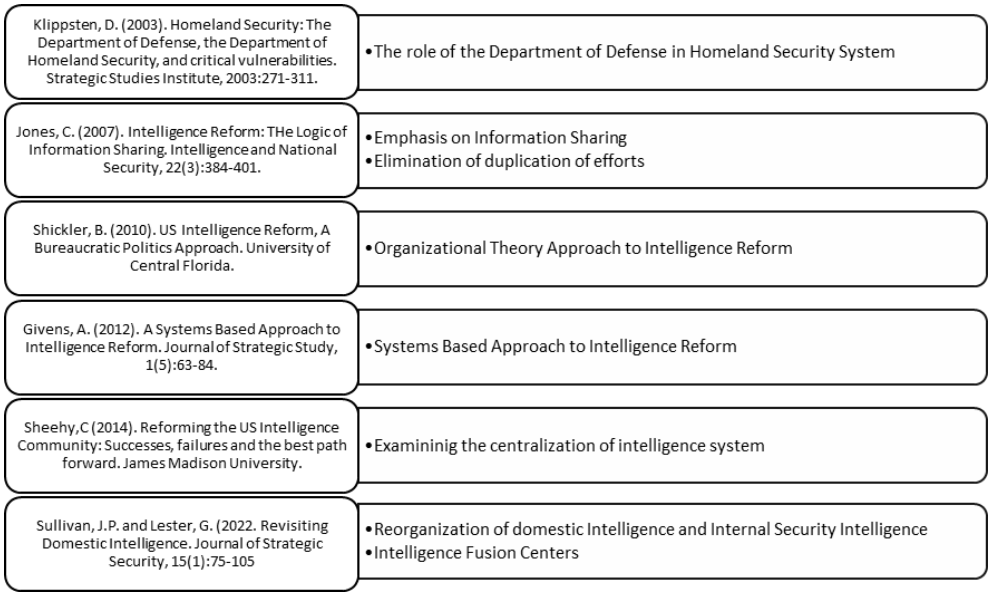
Source: Author

The reforms implemented in America after 09/11, and the performance of the security and defense agencies provide important lessons. Despite extensive academic literature, few researchers have offered useful models for intelligence system reform.

Jones (2007) suggested that a cornerstone of US intelligence reform must be 'information sharing' as a means of adapting to contemporary security challenges. Givens (2012) proposes a systems-based approach to intelligence reform model which enhances effectiveness while reducing the risk of unintended consequences. The research conducted by Givens shows that the benefits of the proposed model manifest themselves primarily in reducing duplication of effort, streamlining operations, and avoiding missteps by anticipating technical and organizational complications (Givens, 2012: 63). While the systems decision pathway suggested above would not necessarily be linear or continually progressive, it presents a hypothetical example of improving intelligence sharing in a holistic way.

Sheehy (2014), on the other hand, examined a model which emphasized the need for centralization, but the study showed that centralization is a "quick fix" that appeases the perceived need for reform but finds difficulty in implementing measurable results, possibly demonstrating a misunderstanding of IC functions (Sheehy, 2014:92). Shickler (2010) offers an organizational theory and a comparative approach to intelligence reform. She indicated that intelligence systems, due to their multifaceted missions and priorities, face far greater challenges than defense systems when it comes to reforming and adapting to new challenges. It is because intelligence systems serve a broader range of missions, face entrenched bureaucratic cultures, operate under secrecy, and deal with rapidly evolving threats, their reform processes are more complex than those of defense systems, which are hierarchical, typically more focused and centralized.

Figure 2: Relevant academic research and models for the intelligence system reform



Source: Author

Of note, most of the publicly available research focuses on only one segment of the intelligence reform process, and, therefore, it is useful to systematically present the most important conclusions that emerge from the examined scientific literature and other relevant sources.

IMPLEMENTATION OF CENTRALIZED VS. DECENTRALIZED INTELLIGENCE SYSTEM

The post-09/11 analysis revealed that one of the major flaws in the intelligence system was poor information sharing among national security components. The main reason for this was the centralization of the intelligence system. Generally, systems and organizations that are centrally organized, have stove-piped structures and overly detailed prescribed procedures (such as decision-making protocols requiring multiple layers of approval) limit many of their processes (Rice, 2004:141). With the aim of improving processes, organizations often implement specific restrictions on themselves, such as information sharing protocols and formal channels of reporting. These limitations often inhibit the development of new capabilities and the incentive to adapt to new circumstances. Therefore, multiple national security experts favor a decentralized intelligence system. They support the creation of an adaptable system that easily accepts and implements changes, has a modular structure, and has fewer restrictive regulations. Each of these options, however, has its advantages and disadvantages (Sheehy, 2014). While centralized systems require (or impose) more precise strategic guidance and better focus in managing collection resources, decentralized systems are more agile, and intelligence sharing is easier.

INTELLIGENCE AND INFORMATION FUSION

After 09/11, the implementation of fusion centers at the state and federal levels represented an attempt to share intelligence across multiple governmental agencies. This organizational structure represented a significant step forward in intelligence operations. It provided certain advantages in circumstances where security threats were constantly changing and developing. Local

and federal fusion centers transformed multiple sources of information into actionable intelligence products. These centers remain an essential element of today's US homeland security system.

Contemporary threats, however, require a combined and cooperative approach. The establishment of such analytical centers at lower (local) levels presents certain challenges. First, the entire philosophy of fusion centers rests on the assumptions of their mutual interaction and connection with the agencies that provide intelligence data and information. But linking hundreds or even thousands of offices, branches, and divisions of security or intelligence agencies through fusion centers is an extensive and time-consuming process (Givens, 2012:66). From an effectiveness perspective, the entire process of intelligence fusion exists to reduce intelligence gaps by integrating intelligence gathered from diverse sources, and, subsequently, to define new intelligence targets more precisely. The fusion center's primary purpose is to "break the bureaucratic culture that, because of resistance to sharing information with others and a desire to pursue its own particular interests, keeps important intelligence information to itself" (Burch, 2006). Some theorists believe that the intelligence service must make a significant shift from its current practices and way of thinking. It is legitimate to protect sources, methods, and raw data, but in today's security environment, the time it takes to protect that data and to produce intelligence reports that are "shareable" can render the data unusable.

ELIMINATING THE DUPLICATION OF EFFORTS AND IMPLEMENTING ALTERNATIVE ANALYTICAL METHODS

Alternative analytical methods to evaluate all assumptions and expand the range of practical solutions. These methods attempt to rise above the generally accepted "herd opinion" – that leads to premature consensus and conclusions. From the above, there is a significant friction between attempts to reduce the level of duplication of intelligence efforts and the implementation of alternative analytical methods. Since security and defense systems are increasingly facing a shortage of personnel, especially in the number of analysts and processes (such as alternative analytical methods, specialization

in a certain narrow area, etc.), which are absolutely necessary to achieve continuous monitoring and to improve the quality of intelligence products, are often eliminated. Faced with the increasing amounts of information that analysts must process, prioritize, and incorporate into intelligence assessments, they often shorten the analytical process to avoid duplication of effort and meet deadlines. Any reform of the intelligence system must consider that properly established analytical processes, an analytical knowledge base, and proven analytical methods, along with collection capacities, are the most valuable organizational resources. Jones (2007:396) explains how to apply similar techniques within the intelligence analysis environment, many of which are well developed in the literature on organizational innovation and learning in conditions of uncertainty. Many scholars recommend using advanced technology to make sense of information as well as providing access to it, through social network analysis, exploratory modeling (used by US Intelligence agencies in Al-Qaeda Threat Assessment post-09/11 to assess the likelihood of future attacks), visualization, and other methods such as use of artificial intelligence and large language models.

A NATIONAL INTELLIGENCE PRIORITIES FRAMEWORK IS A "MUST HAVE"

Changes in the contemporary global security environment are constant, dynamic, unpredictable, and extensive. As such, they present a great challenge to modern security systems, which are struggling with the exponential amount of information that needs processing with the decreasing number of qualified analysts. Therefore, determining and establishing intelligence priorities is one of the key processes. Organizational research increasingly demonstrates that as more information is available, those with superior means of interpretation have a strategic advantage (Jones, 2007:394). Moreover, modern intelligence analytics must respect long-term priorities and respond to short-term intelligence requirements (Pillar, 2007: 151). The complex task of monitoring nuclear proliferation is an example of a long-term priority, while a short-term requirement is a prevention of an imminent attack.

In 2005, the US intelligence community developed and implemented the National Intelligence Priorities Framework (NIPF). It is a framework of "rational and coherent structure that supports analysis, collection and modernization of systems." It also balances resources "to direct them towards priority objectives and intelligence requirements" (Pillar, 2007: 151). It is based on a multidimensional matrix of state and non-state actors on the one hand, and functional processes on the other, while priorities are determined according to the overall role/performance of each actor/process. According to various sources, the NIPF was the most comprehensive mechanism ever implemented within an intelligence system. NATO uses this framework today.

INVESTING IN PERSONNEL DEVELOPMENT IS IMPERATIVE

Selecting, training, and retaining quality intelligence personnel is an ongoing challenge that all developed countries have faced for decades. Although each previous generation of intelligence personnel has struggled with certain challenges, the period after 09/11, emphasizes the criticality of this problem. The need for intelligence personnel who can receive, prioritize, and process the exponentially growing amount of intelligence data and information, apply various analytical techniques and methods, and simultaneously use increasingly sophisticated technical tools is imperative. Training programs must transform from antiquated Cold War approaches and broaden the horizons of intelligence personnel. After 09/11, intelligence committee reports (The Senate Select Committee on Intelligence Report on US Intelligence Community's Pre-09/11 Failure, the House Intelligence Committee's Report on the Joint Inquiry into Intelligence Community Activities Before and After Terrorist Attacks on 09/11, and the 09/11 Commission Report) highlighted the neglect of training and education of intelligence personnel. They stressed general intelligence training was not standardized, creativity of operatives was discouraged, and analyst training was formalized through repetition of certain procedures. Due to these concerns and different analytical methods such as capability analysis, intelligence targeting modeling, pattern or trend analysis, link analysis, temporal analysis, and financial analysis, analysts

were not effective critical thinkers. (Burch, 2006). This research emphasizes an analyst's physical context, exposure to alternative conceptual approaches, availability of diverse search and analysis tools, and informal, low-risk communication allowing the open discussion of tentative ideas (Jones, 2007:394). Developing enough professional intelligence personnel with the right skills is a long-term process that requires careful planning, sustained focus, resources, time, and above all, consistency and patience. Strategic decision-makers and management personnel in the intelligence system must create and encourage an environment in which the continuous development of professional staff occurs. It must also forge an environment where decision makers accept critical and divergent thinking, which includes the toleration of certain risks that intelligence work entails.

MAINTAINING OPTIMAL LEVELS OF SECURITY CLASSIFICATION

Maintaining optimal levels of security classification in intelligence operations is essential for striking a balance between protecting sensitive information and enabling intelligence sharing (Betts, 2007). The detailed process of document classification and declassification is familiar to a relatively limited number of intelligence personnel, and a relatively limited number of end users. Data, information, and reports marked with a certain level of classification are subject to strict legal regulations that restrict their handling. Even in the post-09/11 period, when intelligence and information fusion centers were already in place, problems in sharing this data with those who really needed it continued to exist.

Therefore, decision-makers at strategic levels have issued guidelines for reducing the classification of documents at all levels, except in those situations in which it is justified to maintain a high level of compartmentalization. This is important to protect sources, methods, locations or other sensitive information that could harm the US or the IC if the information is compromised. This does not imply strictly that the state and its security and intelligence services must renounce the principle of secrecy within all security activities. However, it must find a way to respond more quickly and effectively to unpredictable

events through the exchange of intelligence. Furthermore, Held (2004), Posner (2006) and Schneier (2015) in their publications emphasize that states and their security and intelligence services in this new concept of security must be more transparent to the public. They should consider public disclosures when designing, presenting and implementing security policies in accordance with the time and context in which certain risks occur. The disclosures such as white papers and policy reports, annual transparency reports, public hearings and consultations on security regulations and risk assessments and impact statements are essential for fostering transparency, building public trust, and ensuring accountability.

INTELLIGENCE AND INFORMATION SHARING

This tenet of intelligence adaptation and reform is related to the previous one. It is important to emphasize that the term "sharing" primarily depends on an individual agency's organizational attitude and policies, primarily within the agency that collected the information. For example, the National Security Agency (NSA) has extremely strict internal procedures regarding the transfer, handling, and distribution of signals intelligence (SIGINT) data between its organizational units and it enforces rigorous compliance measures. Hundreds of reports, articles, and reviews of the failures of the American intelligence community after 09/11 support the need for more effective "intelligence and information sharing". Relevant data and information must be shared with pertinent participants, processes, or systems (IRTPA, 2004), and the determination of what is relevant lies with several key actors within a state's government, security apparatus, and sometimes international agreements. The process is determined by national security priorities, legal frameworks, and diplomatic considerations.

The crux of the issue is: does information sharing only involve sharing final intelligence reports, or does it also include the necessity of sharing raw intelligence? By analyzing published articles and reports, the following can be concluded. The need for information sharing among and between intelligence agencies is a requirement that most publicly available documents stress as a major shortfall of the US intelligence system. Information sharing

depends mostly on the agency that collected the information. While the literature is concerning whether the necessity of sharing applies only to final products, or to raw data as well, it is realistic to assume that pundits left this issue open for debate. This allows the involved agencies to decide which data, or information, they will share laterally with other intelligence system components, and which ones they will (of course, in order to protect sources, methods, or for some other important reason) still report within the agency's structure.

Almost all intelligence agencies incorporate "information sharing" into their organizational mission, but they share information only in those cases when they are explicitly asked to do so - that is, when they are asked a precise question or for a specific piece of information. Efforts to improve information sharing for national goals have repeatedly failed in transforming intelligence systems. Instead, authors Herman (1998), Betts (2007) and Turner (2015) believe that intelligence organizations can achieve more effective results through better and more precise allocation of areas of responsibility among individual agencies, and by evaluating agency effectiveness solely on information collected within the assigned area of responsibility.

THE DEPARTMENT OF DEFENSE'S ROLE IN THE NATIONAL SECURITY SYSTEM

After 2001, and immediately after the establishment of the Department of Homeland Security, the US Department of Defense's (DoD's) role in homeland defense was vague. Namely, there was no clear distinction between the terms "homeland security" and "homeland defense," so it is not surprising that the DoD's roles and tasks were ambiguous. However, over time (and also prompted by some natural disasters that struck the US, such as Hurricane Katrina), the DoD's role in the homeland security system crystallized DoD's role as defined through several key strategic documents - the US National Security Strategy (NSS), the US National Defense Strategy (NDS), the Strategic Defense Guiidance (SDG), and the National Military Strategy (NMS). These documents provide strategic guidance for the application of national and military power in support of homeland security

(Winslow, 2013:5). The Secretary of Defense still refers to the DoD's tasks in support of homeland security as "homeland defense," emphasizing more than just the semantic difference between the two terms. Defense implies deterrence or response to a threat, while security is a more comprehensive concept in which the DoD participates with other actors. The establishment of the US Northern Command and the more active role of the National Guard are two of the best examples of the active contribution of the US DoD to homeland security. These two examples also represent a shift away from the traditional defense paradigm in the direction of increasing the ability to anticipate threats and prepare for their response (Erchenbrack and Scholer, 2004:3).

THE NEED FOR CONTINUOUS DEVELOPMENT AND TRANSFORMATION OF INTELLIGENCE AND DEFENSE SYSTEMS

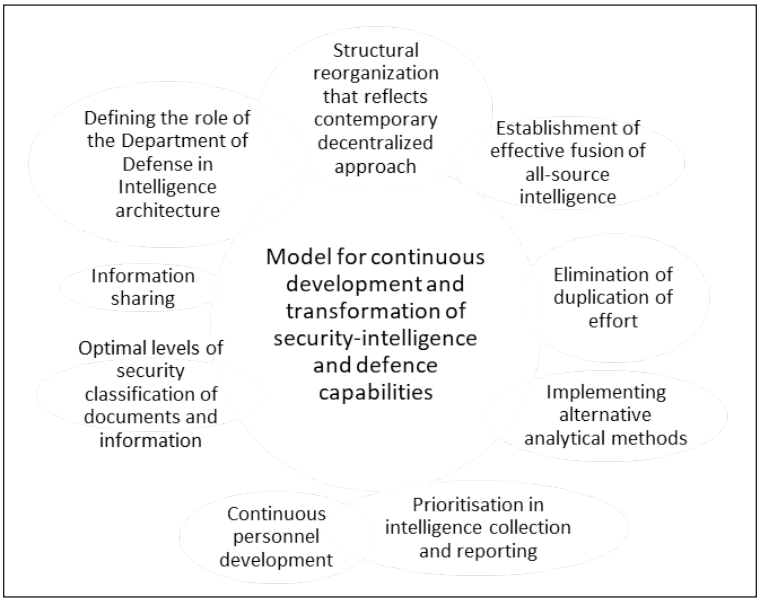
Some of the implemented reforms have taken root, but others have proven ineffective. Major organizational changes implemented in a brief period often create significant problems during their execution. Therefore, when considering these, or any other similar reforms as a starting point for making similar decisions, one must carefully consider all the advantages and disadvantages, and to provide an answer to the following. "Have these changes made the security and defense system more efficient?" "Is America today, after the implemented reforms and because of them, a safer country and more resilient to modern security challenges?" There are metrics to measure success (such as number of terrorist attacks and foiled attrmpts, cyberattack frequency and impact, preparedness and emergency response, public perception and trust etc.), but it's important to remember that these metrics are often influenced by multiple factors, and not all reforms can be easily quantified.

National security related intelligence agencies and armed forces, although often more efficient, are, also significantly more resistant to change than other organizations. Any structural, organizational, or procedural changes in these systems are inherently slow. Legal statutes and other normative

acts, which are restrictive and whose changes are subject to a long bureaucratic procedure, inhibit the speed of change. Organizational rigidity, and inefficient implementation of structural organizational changes creates problems when introducing new business processes. According to Lozančić, the focus of intelligence efforts has shifted from collecting information to managing, prioritizing, and understanding large data and developing predicting capabilities. Therefore, reforming the security intelligence system is vital and should involve all relevant stakeholders (Lozančić, 2020).

According to Bilandžić, most developed countries organize their security intelligence systems to comply with two fundamental principles: centralized management and decentralized functioning (Bilandžić, 2009). In this regard, organizational mechanisms, such as effective data exchange and intelligence oversight and assessment (not necessarily as a corrective componentt, but also a guiding and development-supporting element), and respecting the principle of timeliness are crucial aspects of effective national security intelligence systems.

Figure 3: Proposed model for continuous development and transformation



Source: Author

The contemporary security environment presents threats that modern states face today are extraordinarily complex and require intelligence systems that adapt quickly, prioritize requirements, and are decisive, focused, and persistent. In this context, it is important to emphasize that although the transformation of the intelligence and defense system is often associated with the implementation of new technological achievements and the introduction of new weapons systems, it is important to emphasize that the two are by no means synonymous. Intelligence and defense system transformation must include optimal reorganization, the development of innovative business processes, doctrinal and procedural adaptations and innovations, and the implementation of new technological achievements that will enable better and more efficient operation of the entire system (Foster, 2010:137). Organizational and defense transformation is a demanding and extensive process. Adopting national strategies and policies without clearly outlining steps and responsibilities can negatively impact the process. In

such circumstances, the risk of "strategic failure" increases significantly, while the gap between strategy and real capabilities increases. Even if the desired end state is vague, it is reasonable to expect that the transformation will be successful.

CONCLUSION

Comparing the processes, successes, and failures of other countries can assist in decision-making but may also obscure judgment and reduce objectivity. Therefore, the question "If something is unknown, can it be solved through the examining the past?" is justified. Today's security dilemma is evident, but it does not mean ignoring relevant history is acceptable. In our contemporary security environment, identifying state and non-state adversaries and their intentions is increasingly difficult. A state's intelligence and defense system must be proactive and share experiences and information to address this strategic uncertainty.

The swift progression of events and the short timeliness in which intelligence and defense systems must respond to potential security threats nesessitate the development of predictive capabilities to mitigate these strategic uncertanties. Furthermore, the information revolution of the last decade has exacerbated the problem identified during the Cold War, namely the need to collect and process enormous amounts of data with insufficient human resources.

The transformation of the US security, intelligence, and defense systems after 2001 indicates the need to adapt the government's legal framework for intelligence agencies' collections, differentiating it from domestic police or law enforcement intelligence processes. Domestic law enforcement agencies conduct these operations against a person or group suspected of committing a criminal act. To protect human rights and freedoms, there must be reasonable suspicion, and such actions must be approved by competent, legitimate institutions and established legal processes. However, when collecting national security intelligence data, especially in the context of predicting and preventing hostile threats and actions, it is nearly impossible to precisely determine intelligence collection targets, and it requires mass

collection capabilities. In this sense, most Western countries have adapted their legal frameworks to enable intelligence agencies to collect more efficiently to better detect and prevent an adversary's hostile action. In summary, effective security organizations must learn from the experiences of others. Although the Republic of Croatia is a relatively safe and secure country today, the absence of evidence of a threat is not evidence of the absence of a threat. Therefore, the Croatian national security, intelligence, and defense systems must prepare for future transformations to keep pace with rapid and unpredictable changes within the security environment.

LITERATURE

Books and journal articles:

Betts, Richard K. "The New Politics of Intelligence: Will Reforms Work This Time?" Foreign Affairs 83.3 (2004): 2-8. OmniFile Full Text Mega (H.W. Wilson)

Betts, Richard K. (2007). Enforcing Intelligence: How American Intelligence Services Achieve Effective Results. Columbia University Press.

Bilandžić, M. (2019) Nacionalna sigurnost. Prognoziranje ugroza. Zagreb, Despot Infinitus.

Brown, Michael (2003). Grawe New World: Security Challenges in the 21st century. Georgetown University Press. Washington DC.

Burch, James. "The Domestic Intelligence Gap: Progress Since 9/11?." Homeland Security Affairs, Proceedings of the 2008 Center for Homeland Defense and Security Annual Conference (April 2008).

Davis, L., Pollard, M., Ward, K., Wilson, J., Varda, D. (2010). Long-Term Effects of Law Enforcement's Post- 9/11 Focus on Counterterrorism and Homeland Security. US Department of Justice.

Davies, H.J. Phillip (2012). Intelligence and Government in Britain and the United States. Volume 1: Evolution of the U.S. Intelligence Community. Santa Barbara, California: States. Praeger Security International.

Erckenbrack, A. i Scholer A. (2004). The DOD Role in Homeland Security. National Defense University, Institute for National Strategic Studies.

Foster, Gregory (2010). "Transforming US National Security: A Call for Strategic Idealism." Defense and Security Analysis. Routledge. Vol. 26:2, str. 129-142.

Fox, Ronald (2011). "Defence Acquisition Reform 1960-2009." Center of Military History, Washington DC.

Garamone, J (2016). 9/11 Drove Change in Intelligence Community, NSA Chief Says.

Givens, A (2012). A Systems Based Approach to Intelligence Reform. Journal of Strategic Study, No1 Vol5: 63-84.

Harknett, R., & Stever, J. (2011). The Struggle to Reform Intelligence after 9/11. Public Administration Review, 71(5), str. 700-706.

Held, David. (2004). Global Governance: Power, Interdependence, and Conflict in the 21st Century. Polity Press.

Herman, Michael. (1998). Intelligence Services in the Information Age. Routledge.

Jones, C. (2007). Intelligence Reform: The Logic of Information Sharing. Intelligence and National Security, 22(3): 384-401.

Klippstein, Daniel (2003). Homeland Security: The Department of Defense, The Department of Homeland Security, and critical vulnerabilities. Strategic Studies Institute, 271-311.

Lozančić, Dragan (2020). Insights and Lessons Learned from Croatia's Intelligence Reforms. Security Sector Reform (SSR) in Practice in Europe and Central Asia – No. 1. Geneva Centre for Security Sector Governance

Masse, Todd (2004). The 9/11 Commissioned a National Counterterrorism Center: Issues and Options for Congress.

Negroponte, John & Edward M. Wittenstein, Urgency, Opportunity, and Frustration: Implementing the Intelligence Reform and Terrorism Prevention Act of 2004, 28 Yale L. & Pol'y Rev. (2009).

Posner, Richard A. (2006). Not a Suicide Pact: The Constitution in a Time of National Emergency. Oxford University Press.

Rice, S. (2004). "U.S. National Security Policy Post-9/11: Perils and Prospects." The Fletcher Forum of World Affairs, Vol 28:1, str. 133-144.

Rivkin, Jan and Roberto, Michael and Gulati, Ranjay, Federal Bureau of Investigation, 2007 (March 9, 2010). Harvard Business School Strategy Unit case no. 710-451.

Sandor, F (2019). "The Russian hybrid warfare strategy – neither Russian nor strategy." Defence and Security Analysis.

Sheehy, C. (2014). "Reforming the US Intelligence Community: Successes, failures, and the best path forward." James Madison University.

Shickler, B. (2010). "U.S. Intelligence Reform a Bureaucratic Politics Approach." University of Central Florida.

Schneier, Bruce. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company, 2015.

Sullivan, Sean; Wheeler, Winslow T.; I Korb, Lawrence J. (2010) "Military Reform: An Uneven History and an Uncertain Future," Naval War College Review: Vol. 63: No. 4, Article 19.

Sullivan, J. P., & Lester, G. (2022). "Revisiting Domestic Intelligence." Journal of Strategic Security, 15(1), 75–105.

Thomas, T. (2017). Gerasimov Contemporary Warfare and Current Issues for the Defense of the Country.

Turner, Michael A. (2015). Intelligence and National Security: The Role of Specialization. Palgrave Macmillan.

Uri Bar, J. (2008). Change the Analyst and Not the System: A Different Approach to Intelligence Reform Policy Analysis 4:127-145.

Winslow, T. (2013). "The DoD Role in Homeland Security: Past, Present, and Future." United States Army War College.

Internet sources:

Country comparisons and defence data https://www.iiss.org/publications/the-military-balance/the-military-balance-2018/mb2018-10-country-comparisons-copy, preuzeto 11.02.2024.

Izvješće Obavještajnog odbora SAD-a nakon 11. rujna 2001. Dostupno preko: https://www.9-11commission.gov/report/911Report.pdf

Soa, globalni izazovi. https://www.soa.hr/hr/podrucja-rada/globalni-izazovi/

U.S. Defense Spending compared to other, https://www.pgpf.org/chart-archive/0053_defense-comparison, preuzeto 13.05.2024.

US Defense Science Board Re. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Washington, D.C. 20301-3140port (2003). DoD Roles and Missions in Homeland Security.

US National Commission on Terrorist Attacks: HOW TO DO IT? A DIFFERENT WAY OF ORGANIZING THE GOVERNMENT. Dostupno preko: https://govinfo.library.unt.edu/911/report/911Report_Ch13.htm

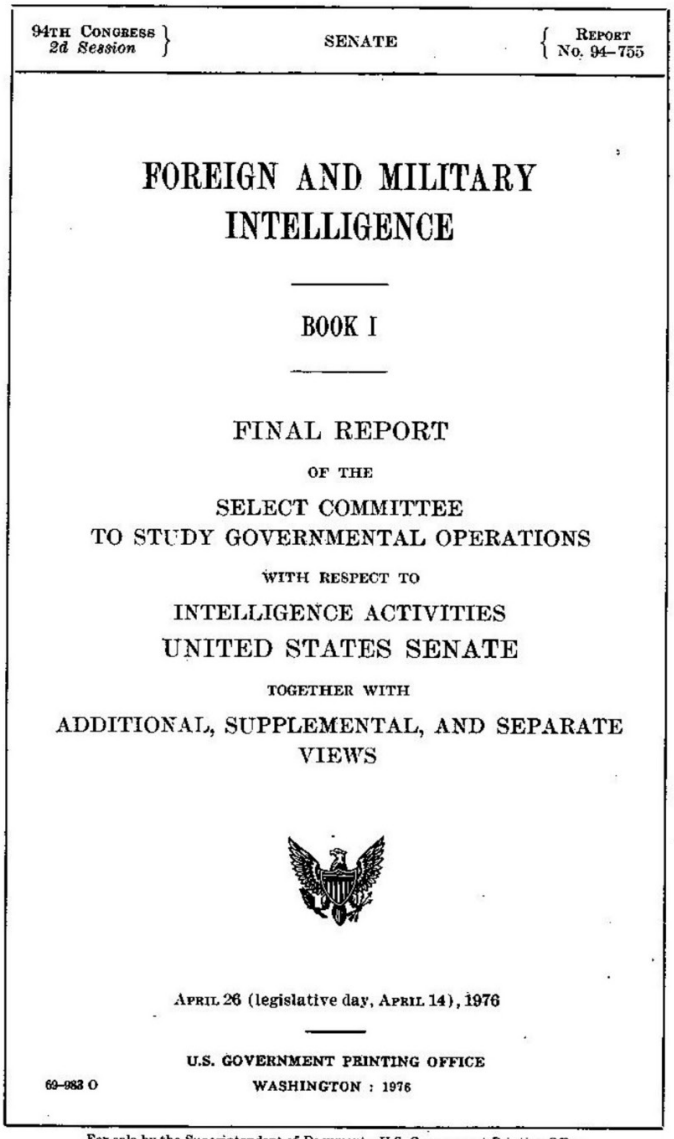
SAŽETAK

Sigurnosni izazovi s kojima se države danas suočavaju složeniji su nego ikad prije. Ovaj rad polazi od temeljne pretpostavke da su pravodobna prilagodba novim sigurnosnim okolnostima i razvoj novih sposobnosti ključni preduvjeti za učinkovito suočavanje suvremenih sigurnosno-obavještajnih i obrambenih sustava s izazovima 21. stoljeća. Korištenjem znanstvenog pristupa, kroz analizu dostupnih znanstvenih istraživanja, kongresnih izvješća i drugih relevantnih dokumenata, na primjeru Sjedinjenih Američkih Država nakon 11. rujna 2001., ovaj rad sustavno prikazuje kako su Sjedinjene Američke Države pristupile reformi nacionalnog sigurnosnog sustava. U završnom dijelu donosi se sinteza stečenih spoznaja i identifikacija ključnih nedostataka u funkcioniranju američkog nacionalnog sigurnosnog sustava. Iz analize se izvode zaključci i prijedlozi koji ukazuju na to da transformacija sigurnosno-obavještajnog i obrambenog sustava mora uključivati njegovu optimalnu reorganizaciju, razvoj novih i unaprjeđenje postojećih poslovnih procesa te implementaciju novih tehnoloških dostignuća koja će omogućiti bolje i učinkovitije funkcioniranje sustava u cjelini.

Ključne riječi:

suvremeni sigurnosni izazovi, reforma sigurnosnog sustava, reforma obrambenog sustava, sigurnosno-obavještajni sustav, nacionalna sigurnost

Cover page of Church Committee report



94TH CONGRESS
2d Session

SENATE

REPORT
No. 94–755

FOREIGN AND MILITARY INTELLIGENCE

BOOK I

FINAL REPORT

OF THE

SELECT COMMITTEE
TO STUDY GOVERNMENTAL OPERATIONS

WITH RESPECT TO

INTELLIGENCE ACTIVITIES
UNITED STATES SENATE

TOGETHER WITH

ADDITIONAL, SUPPLEMENTAL, AND SEPARATE VIEWS

APRIL 26 (legislative day, APRIL 14), 1976

U.S. GOVERNMENT PRINTING OFFICE
69-983 O WASHINGTON : 1976

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402 - Price $5.35

Stock No. 052-071-00470-0