INTELLIGENCE ANALYSIS MODELS FOR ASYMMETRIC THREATS

Ivan R. Dimitrijević[*]
Faculty of Security Studies, University of Belgrade,
Republic of Serbia

Nenad Stekić[**]
Faculty of Security Studies, University of Belgrade,
Republic of Serbia

Abstract: Intelligence analysis in the 21st century, in the light of (post)modern security challenges, vulnerabilities, and threats, is completely adjusted to achieving asymmetric advantage, primarily through development of new techniques and methods for obtaining the data, but also with the use of new and more diverse information sources. New Information and Communication Technologies not only allowed to possible asymmetric threat subjects to increase their capabilities, but also required from nations to adapt their own capacities in new circumstances. The old threat paradigm (Cold War, traditional) asked for appropriate intelligence paradigm based on clear threat(s) holder and relatively known outcome of potential conflict (Mutually Assured Destruction). The new threat paradigm (post-Cold War, post-modern) expanded its focus on the new spectrum of security challenges, vulnerabilities and threats, whose subjects are no longer single nations and their national security capacities. New circumstances are additionally 'aggravated' by the fact that the post-Cold War period is at the same time the age of information and communication technology 'explosion', which certainly and largely effected the increase of academic community interest and stimulated research and development of appropriate intelligence models for the analysis of new threats in the new environment. In that manner, new intelligence analysis knowledge and skills were developed, especially in the context of situation development analysis in contemporary asymmetric conflicts. The most common models used for the asymmetric threat analysis are advanced systems for threat modelling, as well as models for analysis and response to asymmetric threats. In this paper, we present a brief chronological preview of transformation of the "old threat paradigm" into the new threat paradigm, from academic perspective, with recognizing the key elements that affected the

[*] dimitrijevic@fb.bg.ac.rs
[**] nenad.stekic@fb.bg.ac.rs

improvement of national intelligence capacities. Then we gave a preview of some of the most significant intelligence analysis models in the context of new threat paradigm, and we explain their mutual relationship.

Key words: intelligence analysis, asymmetric threats, analytical models, asymmetric advantage.

INTRODUCTION

In the context of (post)modern security challenges, vulnerabilities and threats of the 21st century, the intelligence analysis has been completely adjusted to achieving the asymmetric advantage, primarily through development of new tools and methods for obtaining the data, but also through new and more diverse sources of data needed to design timely and accurate intelligence. The development of Information and Communication Technology (ICT) gave to potential asymmetric threat subjects a possibility to increase their capabilities for attacking the traditional national security actors. The same trend of the ICT development asked from the national security actors, and firstly from intelligence services, to adapt their capacities according to new circumstances.

The old threat paradigm (Cold War, traditional) asked for appropriate intelligence paradigm based on clear threat(s) holder and relatively known outcome of potential conflict (Mutually Assured Destruction), or, according to Thomas Powers, "defining and describing 'the threat' was easier during the forty years of Cold War with the USSR, when estimators at the CIA hammered out the Annual Survey of Soviet Strategic Intentions and Capabilities".[958] On the contrary, the new threat paradigm (post-Cold War, post-modern) expanded its focus to the new spectrum of security challenges, risks, vulnerabilities and threats, whose subjects are no longer single nations and their national security capacities. New circumstances are additionally 'aggravated' by the fact that the post-Cold War period is at the same time the age of information and communication technology 'explosion', which certainly and largely effected the increase of academic community interest and stimulated research and development of appropriate intelligence models for the analysis of new threats in the new environment.

[958] Powers, Thomas, *Intelligence Wars: American Secret History from Hitler to al-Qaeda*, New York Review Books, New York, 2004. Cited in: Vandepeer, Charles, *Rethinking Threat: Intelligence Analysis, Intentions, Capabilities, and the Challenge of Non-State Actors* (Doctoral dissertation), 2011, 53.

In that manner, new intelligence analysis knowledge and skills were developed, especially in the context of situation development analysis in contemporary asymmetric conflicts. The most common models used for the asymmetric threat analysis are advanced systems for threat modelling, as well as models for analysis and response to asymmetric threats. First, we present a brief chronological preview of transformation of the "old threat paradigm" into the new threat paradigm, from academic perspective, with recognizing the key elements that affected the improvement of national intelligence capacities. Then we give a preview of some of the most significant intelligence analysis models in the context of new threat paradigm, and we explain their mutual relationship.

CONCEPTUALIZATION OF ASYMMETRIC THREATS

Notion of asymmetry and the concept of asymmetric threats in academic discourse are not new.[959] According to Bruce Hoffman, these notions appeared in academic literature during the Cold War, although it is commonly claimed that they appeared in the last decade of the 20th century.[960] Asymmetry, because of the factors that causes it, became 'modern' in the contemporary American political thought discourse.[961]

Within the academic conceptualization of asymmetric threats, it is possible to make a distinction between several important "waves" of works.[962] Operationalization of threats in those works does not differ significantly. However, due to the constantly changing contexts in which threats are manifested, there are some inevitably different definitions. Among the most important milestones in expressing the asymmetric threats determinants, we could point out the terrorist attacks of September 11th, 2001, after which the asymmetric threats *de facto* became primary threats related to traditional concepts. Unlike usual targets as economic, military, and political chosen by

[959] According to Cambridge Dictionary, asymmetry/asymmetric is for entity "with two halves, sides, or parts that are not exactly the same in shape and size". See: Cambridge Dictionary, available at: http://dictionary.cambridge.org/dictionary/english/asymmetric (Accessed May 24, 2017)

[960] Hoffman, Bruce and Gordon H. McCormick, „Terrorism, signaling, and suicide attack", *Studies in Conflict & Terrorism* 27, no. 4 (2004): 243-281

[961] Blank, Stephen J. *Rethinking asymmetric threats*, Army war coll strategic studies institute, Carlisle, 2003

[962] Fishbein and Treverton say that there are a so-called 'Cold War wave', then the post-Cold War wave, and finally the wave of post-9/11 papers. See: Warren Fishbein and Gregory Treverton, Making Sense of Transnational Threats, The Sherman Kent Center for Intelligence Analysis, Occasional Papers, Vol.3, No.1, October 2004

state actors, this attack was asymmetric in its nature, because the complete military power of the United States with all its military capabilities, was not able to prevent it.[963]

In his article published right after the 9/11 attacks, Christopher Bellamy said that academic authors had predicted this outcome one decade before it happened.[964] Arreguín-Toft claims that besides the theoretical study of asymmetric conflicts after the Second World War (which was pressured with efforts to develop the new methodology that will enable further theory development), very important segment in asymmetric conflict research is approach focused on selection of actors (strategy), namely explanation of conflict outcome matrix.[965] He makes a distinction between military and academic approaches, claiming that they "ignore each other", which consequently led to, "duplicating the efforts to develop the theory of asymmetric conflicts".[966]

In the most general sense, there were several efforts from academic authors to equalize their viewpoints on asymmetric threats, namely to establish the "Theory of Asymmetric Conflicts". In the same article, Arreguin-Toft argues that the best prediction of asymmetric conflict outcome lies in strategic interaction of conflict actors. His classification of strategies of attack-defence in conflicts, into direct and indirect, namely guerrilla and planned warfare, as two large groups of possible behaviours in conflicts, present one of the first efforts on systematization of asymmetric conflict outcome.[967] Through testing of hypotheses on specific conflict examples, he concluded that the conflict outcome is not determined explicitly by the hard (military) power, but also by the type of strategy used by conflict actors. Thus, it is possible that the weaker side becomes victorious. Therefore, he finds that relative force ratio is not always decisive factor in asymmetric warfare.[968]

---

[963] Bellamy, Christopher. "'Tools of Ill-Omen': The Shifted Conflict Paradigm and Reduced Role of Conventional Military Power." *Cambridge Review of International Affairs* 15, no. 1 (2002): 152

[964] Ibid, 149

[965] Arreguin-Toft, Ivan. "How the weak win wars: A theory of asymmetric conflict." *International Security* 26, no. 1 (2001): 93-128

[966] Ibid, 101.

[967] Ibid.

[968] According to findings by Arreguin-Toft, military superior adversary will win in the conflict if the same strategy is used in 76% of conflicts, while weak adversary will win in 63% if interactions between different types of strategies are achieved. See: Arreguin-Toft, Ivan. "How the weak win wars: A theory of asymmetric conflict". *International Security* 26, no. 1 (2001), 111

The nature of asymmetric threats largely depends on the perception of the object of those threats. Bellamy says that the Western civilization is specifically fertile ground for implementation and exploitation of asymmetric threats "because of all its inherent vulnerabilities", such as huge concentration of a large number of people in one place, freedom of movement of people and capital, developed mass media and fast information transmission in digital world.[969] The new environment in the context of post-9/11 threats is not suitable for aforementioned description. Namely, in the Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001, by the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, published in December 2002, *asymmetry*, and *asymmetric threats* are not mentioned even once.[970]

In the article *Threat-perception and the Armament-Tension Dilemma* published in 1958, author David Singer presented his threat model as a sublimation of initial efforts on conceptualization of threats in the literature at that time. He starts from the fact that the International Relations system was bipolar with clearly expressed military threat. In such a system, state actors perceive threat according to the quasi-mathematical model, which says that such threat perception is equal to the product of assessed possibilities and assessed intention.[971] Taking this course of argumentation, Robert Steele provided classification of threats into violent state, violent non-state, non-violent non-state and violent mixed threats.[972] New (post-Cold War, post-modern) threat paradigm expanded its focus to new spectrum of security challenges, vulnerabilities, and threats, whose actors are no longer states and their national security capabilities. In the context of new threat paradigm, authors like Bellamy and Stephen Blank claim that not much has essentially changed. What is specific for the 9/11 attack is the fact that it marked the end of the Cold War forever, and introduced new asymmetric threats.[973] Bellamy believes that "New York and Washington have experienced now (2001) what the world has survived for decades, such as aircraft hijackings and attacks in urban areas".[974]

---

[969] Op. cit. Christopher Bellamy, 153

[970] Integral version of document is available at: https://fas.org/irp/congress/2002_rpt/911rept.pdf (Accessed on May 23rd, 2017)

[971] Singer, J. David. "Threat-perception and the armament-tension dilemma". *Journal of Conflict Resolution* 2, no. 1 (1958): 90-105

[972] Steele, Robert D. (2002). *The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats*. Strategic Studies Institute, U.S. Army War College, Carlisle, p.12

[973] Ibid. Christopher Bellamy, p.157

[974] Ibid.

Vandepeer says that Singer's definition of threat significantly determined not only further research within the scientific community in the USA and (former) USSR, but also had a deeper impact on defence policies of superpowers in the Cold War constellation.[975] Although it is the first model almost universally accepted and applied in the academic literature dealing with intelligence and assessment of state and non-state threats[976], this model was severely criticized by the academic community.

Among the most comprehensive academic criticisms of Singer's model, Vandepeer gives a problem of measuring indicators of "intention" and "capabilities", as elements of threat.[977] As an example, the National Security Strategy of the USA was used, which moved its focus from state to non-state threats, changing at the same time the ways for measuring indicators. In that sense, Vandepeer gives possibilities (Singer's "capabilities") for threat achievement with use of conventional weapons, chemical, biological, radiological and nuclear (CBRN) weapons, weapons of mass destruction, as well as other means for use of armed force. Contemporary technology enabled non-state actors an easy access to the weapons mentioned above, and use with almost the same effect as if it were used by state actors. [978] Finally, he states that basic indicators of "capabilities" are actually the people, because without people it is not possible to carry out an attack, and thus to measure precisely the indicators of intentions and possibilities for manifestation of threat.[979]

REVIEW OF INTELLIGENCE ANALYSIS MODELS FOR ASYMMETRIC THREATS

For appropriate response to asymmetric threats, as already pointed out, certain means are needed for political decision-makers to be informed for achieving the asymmetric advantage. Since it is evident that "the predominant characteristic of non-traditional and asymmetric threats is their very character - *not* traditional, *not* symmetric"[980], what was recognized as a key competence

---

[975] Vandepeer, Charles, *Rethinking Threat: Intelligence Analysis, Intentions, Capabilities, and the Challenge of Non-State Actors* (Doctoral dissertation), 2011
[976] Ibid.
[977] Vandepir navodi i da se kritika Singerovog modela vrlo brzo pokazala osnovanom, i u praksi. Videti više u: Vandepeer, Charles, *Rethinking Threat: Intelligence Analysis, Intentions, Capabilities, and the Challenge of Non-State Actors* (Doctoral dissertation), 2011
[978] Ibid.
[979] Ibid.
[980] Steele, Robert D. (2002). *The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats*. Strategic Studies Institute, U.S. Army War College, Carlisle, p. 40

of future decision-makers and intelligence professionals who will inform them, is *conceptual flexibility*, according to Steven Metz[981] and Max Manwaring[982].

It is the main reason why it is essential for the *new craft of intelligence* to become a key factor in achieving the asymmetric advantage against non-traditional threats.[983] The new craft of intelligence means adjusting to the new context and improvement of intelligence analysis as the only mechanism for achieving the asymmetric advantage in the 21st century. As already pointed out, new circumstances are additionally 'aggravated' by the fact that the post-Cold War period is at the same time the age of information and communication technology 'explosion', which certainly and largely effected the increase of academic community interest and stimulated research and development of appropriate intelligence models for the analysis of new threats in the new environment. In that manner, new intelligence analysis knowledge and skills were developed, especially in the context of situation development analysis in contemporary asymmetric conflicts.

Surely, what remain as constant in contemporary intelligence analysis, are the standard analytical techniques that allow us to understand the use value of different models for asymmetric threats analysis. Thus, Hank Prunkcun recognizes three key analytical techniques that have to shape planning of prevention, preparedness, response and recovery (PPRR) regarding the asymmetric threats.[984] Those are threat analysis, vulnerability analysis, and risk analysis, which could be summed through the following steps:

1. "Identify the threat(s);
2. Explore vulnerabilities to this threat(s);
3. Gauge the likelihood that the threat(s) will eventuate;
4. Assess the consequence the threat will have; and
5. Construct a PPRR plan".[985]

In addition, models for asymmetric threats analysis which are already developed, are used in accordance with the 'level of analysis' on which the

---

[981] Manwaring, Max (2001). *Internal Wars: Rethinking Problem and Response*, Studies in Asymmetry, Carlisle Barracks: Strategic Studies Institute, September 2001, p. 76

[982] Metz, Steven (1993). *The Future of Insurgency*, Carlisle Barracks: Strategic Studies Institute

[983] Steele, Robert D. (2002). *The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats*. Strategic Studies Institute, U.S. Army War College, Carlisle, p. 40

[984] Although Prunckun presented these techniques in the context of counter-terrorism, they are applicable to the whole scope of contemporary asymmetric threats

[985] Prunckun, Hank, *Handbook of Scientific Methods of Inquiry for Intelligence Analysis*. Lanham: The Scarecrow Press, 2010

given intelligence analysis functions. *Strategic intelligence* is focused on the long-term estimations in international relations, primarily for great powers, so these models are practically not applicable to this level, but could be used for predictions of certain trends for larger periods. *Operational intelligence* provides support to an operation that is either underway or about to begin.[986] *Tactical intelligence* is short-term and time-limited, and it contributes directly to the achievement of an immediate goal.[987] Certainly, there are different models in intelligence analysis, developed and used for threat analysis and assessment. Robert M. Clark gives his taxonomy of the existing models used in intelligence.[988] He divides them into two main groups – generic and combined models. Generic model includes lists, curves, comparative modelling (Benchmarking), pattern models, relationship models, profiles, process models, and simulation models. Combined models are geospatial models, human terrain models, space-time models, and geographic profiling. The most common models used for the asymmetric threat analysis are advanced systems for threat modelling, as well as models for analysis and response to asymmetric threats and models for ontological analysis of threats and vulnerabilities. We are going to give a review of some of the most significant intelligence analysis models in the context of new threat paradigm, and explain their mutual relationship and possible applications.

Adaptive Safety Analysis and Monitoring System (ASAM) was developed in 2004 by researchers from the University of Connecticut, and it represents a software tool "which has to assist intelligence analysts to identify asymmetric threats, to predict possible evolution of the suspicious activities, and to suggest strategies for countering threats."[989] The goal of the ASAM system is to combine information about the adversary obtained from different intelligence services, in order to improve our understanding of their capabilities and prevent possible attacks.[990] Like many other tools for asymmetric threats assessment, ASAM is based on Bayesan probability, namely on Bayesan networks and on Hidden Markov Model. This system is created mainly for asymmetric threats, for "tactics employed by some

---

[986] Ibid.
[987] Ibid.
[988] Clark, Robert, *Intelligence Analysis: A Target-Centric Approach*. London: Sage, 2013
[989] Singh, Satnam, Allanach, Jeffrey, Tu, Haiying, Pattipati, Krishna, & Willett, Peter (2004, October). Stochastic Modeling of a Terrorist Event via the ASAM System. In *Systems, Man and Cybernetics, 2004 IEEE International Conference on* (Vol. 6, pp. 5673-5678). IEEE. Also: Singh, Satnam, Donat, William, Tu, Haiying, Lu, Jijun, Pattipati, Krishna, & Willett, Peter (2006, October). An Advanced System for Modeling Asymmetric Threats. In *Systems, Man and Cybernetics, 2006. SMC'06. IEEE International Conference on* (Vol. 5, pp. 3943-3948). IEEE
[990] Ibid.

countries ("rogue and/or failed states"), terrorist groups, or individuals to carry out attacks on a superior opponent while trying to avoid direct confrontation."[991]

Using similar methodologies, Robert Popp and associates[992] presented in 2004 the collaborative environment with the goal of integrating and sharing information between different existing tools for modelling, named *Network Modelling Environment for Structural Intervention Strategies (NEMESIS)*. Tools used for NEMESIS are aforementioned ASAM system and *Organizational Risk Analysis (ORA)*.

Researchers from University of Arizona[993] presented in 2010 the software package named *Asymmetric Threat Response and Analysis Program (ATRAP)*, which consists of "set of tools for annotating and automatically extracting entities and relationships from documents, visualizing this information in relational, geographic, and temporal dimensions, and determining future courses of action of adversaries by creating situational threat templates and applying customized prediction algorithms."[994] ATRAP is based on databases, and its main advantage is that, besides structured data, it processes unstructured data (text) through *Natural Language Processing (NLP)*.

Eric Little and Galina Rogova considered ontological[995] analysis of threats and vulnerabilities[996], with special focus on asymmetric threats. Authors start from the viewpoint that the "threat is a very complex ontological item and, therefore, a proper threat ontology must be constructed in accordance with… the complexities of the objects, object attributes, processes, events, and relations that make up these states of affairs."[997] That is why they suggest basic metaphysical concepts which are necessary for threat ontology construction, and give "…a formal ontological structure of threats as

---

[991] Ibid.

[992] Popp, Robert, Pattipati, Krishna, Willett, Peter, Serfaty, Daniel, Stacy, Webb, Carley, Kathleen, Allanach, Jeffrey, Tu, Haiying & Singh, Satnam, "Collaboration and Modeling Tools for Counter-Terrorism Analysis". In *Computational Intelligence for Homeland Security and Personal Safety, IEEE, 2004:* 46-52

[993] Chan, Erwin, Ginsburg, Jason, Ten Eyck, Brian, Rozenblit, Jerzy, and Mike Dameron, "Text Analysis and Entity Extraction in Asymmetric Threat Response and Prediction." In *International Conference on Intelligence and Security Informatics, IEEE, May 2010,* 202-207

[994] Ibid, 202

[995] *Ontology,* in IT terminology, stands for formally defined system of notions and/or concepts, and relations between those notions/concepts.

[996] Little, Eric G., & Galina L. Rogova, An Ontological Analysis of Threat and Vulnerability. In *9th International Conference on Information Fusion, July 2006, IEEE,* 1-8

[997] Ibid, 7

integrated wholes possessing three inter-related parts: intentions, capabilities and opportunities, and shows how these elements stand to one another, as well as to conditions of vulnerability."[998]

Besides the mentioned analysis models, in military intelligence there are various methods and techniques used for the *Situation Development analysis*, both for conventional and unconventional warfare (asymmetric, counterinsurgency, urban areas warfare, etc.). Briefly, "Situation Development is an ongoing process carried out by a team led by intelligence analysts to estimate current and future threats to friendly forces, the local populace and host nation government interests within a unit's area of operation and with respect to the current and planned friendly-force missions."[999] Within Situation Development, a significant tool is *Asymmetric Threat Matrix (ATM)*, with the purpose "to identify most probable, feasible, dangerous and likely enemy courses of action in order to prioritize force protection effort in the area of operations."[1000] This matrix specifies every threat within the enemy course of action, as a complex of four factors:

1. Prevalence of threat, which is assigned to a given enemy group (terrorists, insurgents, criminal groups, etc.);
2. Likelihood of achieving enemy goals (immediate, not long-turn goals);
3. The number of people likely to be potentially reachable by attack, related to the avenue of approach (air, land, water, cyber, etc.);
4. Ease of acquisition and use of means for attack, related to the delivery system.[1001]

Bearing in mind the fact that these factors are multiplied and expressed numerically through previously given values, this method could be viewed as a risk assessment of the enemy course of action, because the value is given as a product of sums of severity of consequences, and probability for those consequences to occur.

---

[998] Ibid, 7

[999] Powell, Gerald M., Matheus, Christopher J., Ulicny, Brian, Dionne, Robert, Kokar, Mieczyslaw M., & Lorenz, David (2008, June). An Analysis of Situation Development in the Context of Contemporary Warfare. In *Proc. of the 13th International Command and Control Research and Technology Symposium, Seattle, WA*, 2-3

[1000] Ibid, 3

[1001] Ibid, 4

Other authors also used risk assessment for development of the models for response to terrorist threat. Elisabeth Paté-Cornell and Seth Guikema presented the Probabilistic Model for Terrorist Threats, aimed at threat and countermeasures prioritization from the system analysis perspective.[1002] The model they developed is based on probabilistic risk analysis, decision analysis, and elements of game theory, and could account for the probabilities of different scenarios. The goal of development of this model is bringing the order into large quantities of information available, and description of links between the core elements of different classes of scenarios.

Finally, in asymmetric threat intelligence analysis, there are different simulation models used, which are a valuable asset because for analysis, observation, and prediction of behaviour of different actors, they are less expensive, could be repeated, and tested on various scenarios.[1003] Among these models, we could single out the Counter-Terrorism Simulation Framework developed on the OODA loop. [1004] The essence of OODA loop is that it "…implies that the decision making cycle is shortened and faster than the enemy's. In this way, the enemy is constantly late after the actions of the 'faster' side in conflict, and in time there will be an absence of appropriate response to a new situation, and he is becoming ineffective and disorganized".[1005] It is this methodology that enabled the authors of Counter-Terrorism Simulation Framework to solve the following common issues in modelling terrorist threats: (1) because of the large amount of intelligence data from various sources, that are mostly not well organized, there are multiple parameters to be considered at the same time; (2) in order to use predictive and preventive advantages of counter-terrorism simulation techniques and tools in the best way, timely availability of information from various sources, is essential, and (3) it is necessary to avoid false alarms or false confirmations to ensure information authenticity."[1006]

Based on the application of OODA loop in the existing simulation models for counterterrorist threats, a framework was suggested, which includes the introduction of two key novelties related to intelligence agencies.

[1002] Paté-Cornell, Elisabeth, & Seth Guikema, „Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities among Countermeasures." *Military Operations Research 7*, 4(2002): 5-23

[1003] Tajwer, Khaula, & Shamsi, Jawwad, "Counter-Terrorism Simulation Network", *IEEE International Conference on Information and Emerging Technologies*, IEEE, 2010, 1

[1004] OODA (Observation, Orientation, Decision and Action) cycle was developed by John R. Boyd.

[1005] Mandić, Velimir, "Manevarski pristup operacijama". *Novi glasnik 2/2016*, 43

[1006] Tajwer, Khaula, & Shamsi, Jawwad, "Counter-Terrorism Simulation Network", *IEEE International Conference on Information and Emerging Technologies*, IEEE, 2010, 1

The first one is setting up a functional communication between intelligence services and other state services and institutions important to national security. The second one is the introduction of centralized intelligence database and process of information acquisition, where the OODA loop was applied. [1007] In this manner, the more realistic and authentic information could be provided, in space and time, for counterterrorist simulations and tools.

CONCLUSION

The application of these models within the asymmetric threats intelligence analysis has a wide scope, so those models could practically be applied for the widest possible spectrum of actual contemporary security threats, like fight against terrorism, counterinsurgency, urban areas fighting, etc.[1008] The essence of using the presented models is to empower intelligence analysts with the "ability to find pertinent data faster, conduct more efficient and effective analysis, share information with others, relay concerns to the appropriate decision-makers, and support them with better information to make effective decisions."[1009] This is especially important in the 21st century, where the amount of data available is enormous and asks for more time dedicated to collection than for analysis, so the available tools are the way to preserve the quality of intelligence analysis of asymmetric threats with efficient time management, and thus provide relevant, appropriate, and timely information to decision-makers as fast as possible.

The added value of the development of presented models are the conclusions with recommendations which, if applied, could significantly improve not only the content and quality of intelligence analysis, but also the means in which intelligence services (especially within large intelligence communities with numerous agencies and organizations) are exchanging data with the biggest possible time saving and the most efficient management of the existing human

---

[1007] Ibid, 3-5

[1008] Hank Prunckun, for example, recognizes 'threat communities' in contextualization of contemporary threats for intelligence analysis, and within 'external communities' he includes: criminals and criminal groups, international and transnational terrorists, insurgents and guerrillas, domestic anarchists, cyber law breakers, rights campaigners, spies-for-hire, foreign intelligence services. In: Prunckun, Hank, *Handbook of Scientific Methods of Inquiry for Intelligence Analysis*, The Scarecrow Press, Lanham, 2010, 167

[1009] Popp, Robert, Pattipati, Krishna, Willett, Peter, Serfaty, Daniel, Stacy, Webb, Carley, Kathleen, Allanach, Jeffrey, Tu, Haiying & Singh, Satnam (2004, July). Collaboration and Modeling Tools for Counter-Terrorism Analysis. In *Computational Intelligence for Homeland Security and Personal Safety, 2004. CIHSPS 2004. Proceedings of the 2004 IEEE International Conference,* 46

and technological (primarily Information and Communication technology) resources. That is why it is not necessary to emphasize the importance of academic community for the development of the asymmetric threats analysis models, which in previous decades has made big efforts to research all the possible ways for application of the existing techniques, tools, and methods from natural, technical and social sciences and scientific disciplines, onto the improvement of the intelligence analysis process and intelligence work as a whole.

LITERATURE

1. Arreguín-Toft, Ivan. "How the Weak Win Wars: A Theory of Asymmetric Conflict." International Security 26(2001): 93-128
2. Bellamy, Christopher. "'Tools of Ill-Omen': The Shifted Conflict Paradigm and Reduced Role of Conventional Military Power." Cambridge Review of International Affairs 15, no. 1 (2002): 149-157
3. Blank, Stephen J. Rethinking Asymmetric Threats. Carlisle: Strategic Studies Institute, U.S. Army War College, 2003
4. Chan, Erwin, Ginsburg, Jason, Ten Eyck, Brian, Rozenblit, Jerzy, and Mike Dameron, "Text Analysis and Entity Extraction in Asymmetric Threat Response and Prediction". In International Conference on Intelligence and Security Informatics, IEEE, May 2010, 202-207
5. Clark, Robert, Intelligence Analysis: A Target-Centric Approach. London: Sage, 2013.
6. Hoffman, Bruce, and Gordon H. McCormick. "Terrorism, signalling, and suicide attack." Studies in Conflict & Terrorism 4(2004): 243-281
7. Little, Eric G., & Galina L. Rogova, „An Ontological Analysis of Threat and Vulnerability". In 9th International Conference on Information Fusion, July 2006, IEEE, 1-8
8. Mandić, Velimir, „Manevarski pristup operacijama". Novi glasnik 2/2016, 39-69
9. Manwaring, Max, Internal Wars: Rethinking Problem and Response. Studies in Asymmetry, Strategic Studies Institute, September 2001
10. Metz, Steven, The Future of Insurgency. Strategic Studies Institute, 1993
11. Paté-Cornell, Elisabeth, & Seth Guikema, „Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities among Countermeasures. "Military Operations Research 7, 4(2002): 5-23

12. Popp, Robert, Pattipati, Krishna, Willett, Peter, Serfaty, Daniel, Stacy, Webb, Carley, Kathleen, Allanach, Jeffrey, Tu, Haiying & Singh, Satnam, „Collaboration and Modeling Tools for Counter-Terrorism Analysis.“ In Computational Intelligence for Homeland Security and Personal Safety, IEEE, 2004: 46-52
13. Powell, Gerald M., Matheus, Christopher J., Ulicny, Brian, Dionne, Robert, Kokar, Mieczyslaw M., & Lorenz, David, „An Analysis of Situation Development in the Context of Contemporary Warfare.” Proceedings of the 13th International Command and Control Research and Technology Symposium, Seattle, WA, June 2008
14. Powers, Thomas, Intelligence Wars: American Secret History from Hitler to al-Qaeda, New York Review Books, New York, 2004
15. Prunckun, Hank, Handbook of Scientific Methods of Inquiry for Intelligence Analysis, The Scarecrow Press, Lanham, 2010
16. Singer, J. David. „Threat-perception and the armament-tension dilemma.” Journal of Conflict Resolution 2, 1(1958): 90-105
17. Singh, Satnam, Allanach, Jeffrey, Tu, Haiying, Pattipati, Krishna, & Willett, Peter, „Stochastic Modeling of a Terrorist Event via the ASAM System“, IEEE International Conference on Systems, Man and Cybernetics, Vol. 6, 2004, 5673-5678
18. Singh, Satnam, Donat, William, Tu, Haiying, Lu, Jijun, Pattipati, Krishna, & Willett, Peter, „An Advanced System for Modeling Asymmetric Threats“, IEEE International Conference on Systems, Man and Cybernetics, Vol. 5, 2006, 3943-3948
19. Steele, Robert D., The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats. Strategic Studies Institute, U.S. Army War College, Carlisle, 2002
20. Tajwer, Khaula, & Shamsi, Jawwad, „Counter-Terrorism Simulation Network“, IEEE International Conference on Information and Emerging Technologies, IEEE, 2010, 1-6.
21. Vandepeer, Charles, Rethinking Threat: Intelligence Analysis, Intentions, Capabilities, and the Challenge of Non-State Actors (Doctoral dissertation), 2011
22. Warren Fishbein and Gregory Treverton, Making Sense of Transnational Threats, The Sherman Kent Center for Intelligence Analysis Occasional Papers, 3(1), October 2004

MODELI ZA OBAVEŠTAJNU ANALIZU ASIMETRIČNIH PRETNJI

Ivan R. Dimitrijević[*]
Fakultet bezbednosti, Univerzitet u Beogradu,
Republika Srbija

Nenad Stekić[**]
Fakultet bezbednosti, Univerzitet u Beogradu,
Republika Srbija

Apstrakt: Obaveštajna analiza je u 21. veku, u svetlu (post)modernih bezbednosnih izazova, ranjivosti i pretnji, potpuno prilagođena ostvarivanju tzv. asimetrične prednosti, prvenstveno kroz razvoj novih tehnika i metoda dolaženja do podataka, ali i kroz upotrebu novih i raznovrsnijih izvora informacija. Nove informacione i komunikacione tehnologije nisu omogućile samo potencijalnim nosiocima asimetričnih pretnji da povećaju svoju sposobnost, već su zahtevale i od država da usklađuju sopstvene kapacitete u novonastalim okolnostima. Stara (hladnoratovska, tradicionalna) paradigma pretnji, iziskivala je i adekvatnu obaveštajnu paradigmu zasnovanu na jasnom nosiocu pretnje ili pretnji i relativno poznatom ishodu potencijalnog konflikta (sigurno uzajamno uništenje). Nova (posthladnoratovska, postmoderna) paradigma pretnji proširila je svoj fokus na novi spektar bezbednosnih izazova, ranjivosti i pretnji čiji nosioci više nisu samo države i kapaciteti njihove nacionalne bezbednosti. Nove okolnosti dodatno su „otežane“ činjenicom da je posthladnoratovski period istovremeno i doba svojevrsne eksplozije informacionih i komunikacionih tehnologija, što je nesumnjivo, u velikoj meri uticalo na povećanje interesovanja akademske zajednice i podsticanje istraživanja i razvoja odgovarajućih obaveštajnih modela za analizu novih pretnji u novim okolnostima. U tom pogledu razvijena su nova znanja i veštine za obaveštajnu analizu, a posebno u kontekstu analize razvoja situacije u savremenim asimetričnim sukobima. Najčešći modeli koji se koriste za analizu asimetričnih pretnji su napredni sistemi modeliranja ovih pretnji, kao i modeli za predviđanje i odgovor na asimetrične pretnje. U radu se, kroz kratki istorijski pregled transformacije tzv. stare paradigme pretnji u novu, prepoznaju ključni elementi koji su uticali na unapređenje obaveštajnih

[*] dimitrijevic@fb.bg.ac.rs
[**] nenad.stekic@fb.bg.ac.rs

kapaciteta država, kao reakcije na ovu transformaciju. Zatim je pružen pregled nekih od najznačajnijih modela obaveštajne analize u kontekstu nove paradigme pretnji i objašnjen je njihov međusobni odnos.

Ključne reči: obaveštajna analiza, asimetrične pretnje, analitički modeli, asimetrična prednost.