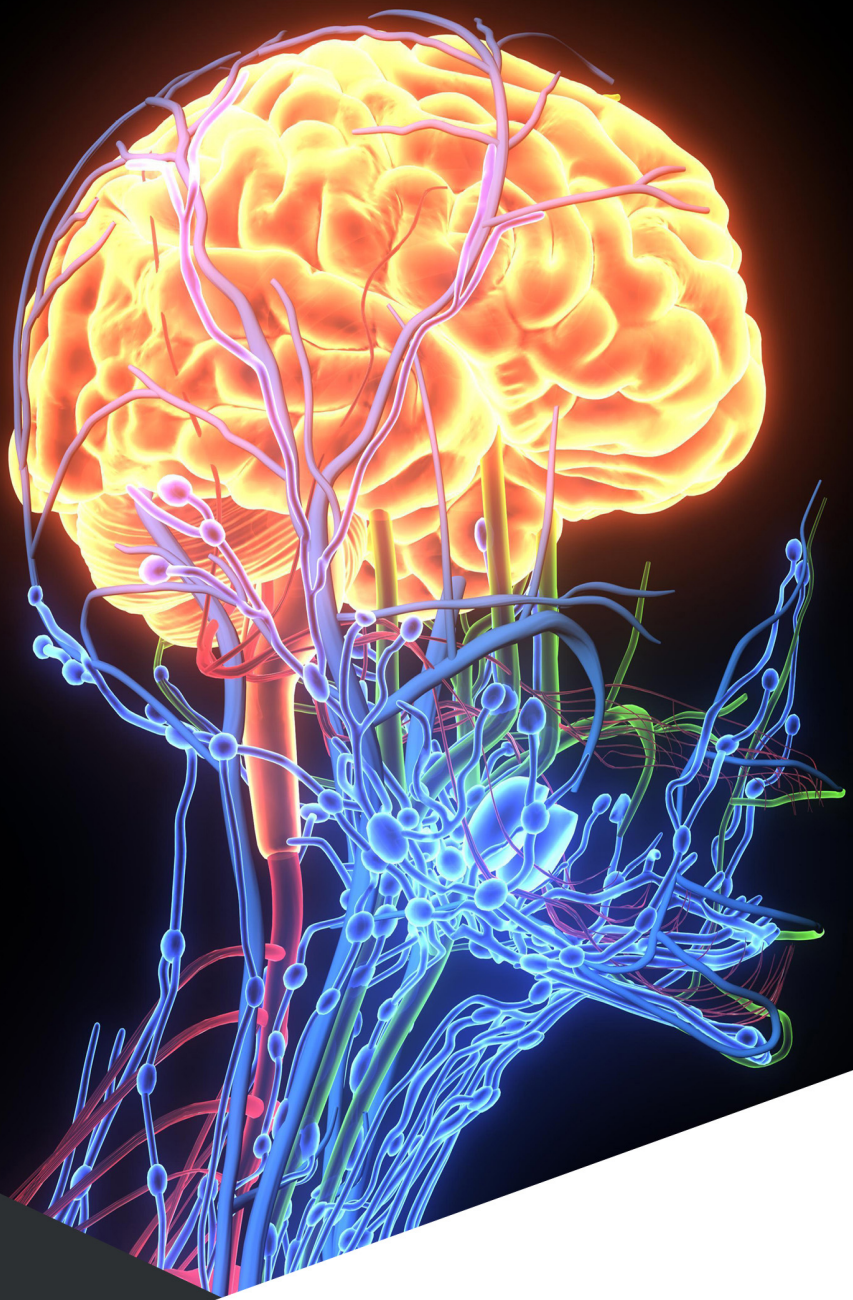
eISBN: 978-1-68108-411-4
ISBN: 978-1-68108-412-1

THE ANATOMY OF COUNTERINTELLIGENCE: EUROPEAN PERSPECTIVE



Editors:
Iztok Podbregar
Teodora Ivanuša

Bentham Books

The Anatomy of Counterintelligence: European Perspective

Edited by:

Iztok Podbregar
Faculty of Organizational Sciences
University of Maribor
Kranj
Slovenia

&

Teodora Ivanuša
Faculty of Logistics
University of Maribor
Celje
Slovenia

The Anatomy of Counterintelligence: European Perspective

Editors: Iztok Podbregar & Teodora Ivanuša

ISBN (eBook): 978-1-68108-411-4

ISBN (Print): 978-1-68108-412-1

First published in 2016.

advertisements or ideas contained in the Work.

Limitation of Liability:

In no event will Bentham Science Publishers, its staff, editors and/or authors, be liable for any damages, including, without limitation, special, incidental and/or consequential damages and/or damages for lost data and/or profits arising out of (whether directly or indirectly) the use or inability to use the Work. The entire liability of Bentham Science Publishers shall be limited to the amount actually paid by you for the Work.

General:

1. Any dispute or claim arising out of or in connection with this License Agreement or the Work (including non-contractual disputes or claims) will be governed by and construed in accordance with the laws of the U.A.E. as applied in the Emirate of Dubai. Each party agrees that the courts of the Emirate of Dubai shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this License Agreement or the Work (including non-contractual disputes or claims).
2. Your rights under this License Agreement will automatically terminate without notice and without the need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.
3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Ltd.
Executive Suite Y - 2
PO Box 7917, Saif Zone
Sharjah, U.A.E.
Email: subscriptions@benthamscience.org

CONTENTS

FOREWORD 1

The complexity of the contemporary security environment and the growth of information society present us with important dilemmas in how to effectively protect key national intelligence and information, given that timely and accurate information has become an important part of achieving strategic interests. After the fall of the Berlin Wall, the international community was lulled into a false perception that counter-intelligence was no longer needed, since we were in an era of supposedly open and friendly relations. This has been proven wrong, and we have recently seen that even closest allies pursue intelligence activities against each other. In order to detect these risks and threats, we need counter-intelligence— alongside security it provides the most complex defense of national strategic interests. The transitional countries of Europe, among them the Balkan states, have not paid sufficient attention to the field of counter-intelligence in the building of their own national security systems. Because anything related to past systems of national security was abolished, forgotten, or overlooked, the national security of these states was negatively impacted; furthermore, they are now faced with having to look for an adequate and effective model of counter-intelligence. In doing so, they are sometimes unaware of the important differences between various counter-intelligence models, which were adapted to different countries and environments. This is why transitional countries should begin by looking at their own context and especially at the European perspective, even though the American perception of counter-intelligence is perhaps more immediately accessible through open sources.

The present book is an excellent foundation for building a comprehensive European concept of counter-intelligence and for further pursuit of professional and scientific approaches in the field of counter-intelligence, in particular European counter-intelligence. The added quality of the text is the integration of practical knowledge and experience, the comparison between European, in particular Balkan, and American perspectives, and the comparison of counter-intelligence models in different regions.

Dr. Denis Čaleta
Institute of Corporative Security Studies
Slovenia

FOREWORD 2

Contemporary threats to national security are more complex, less predictable, and harder to detect than ever, with foreign intelligence services playing an increasingly aggressive, thorough, and effective role in pursuing foreign national interests on both regional and global levels. This calls for a paradigm shift in the theory and practice of counter-intelligence.

This book presents a comprehensive, coherent, and at the same time alternative image of counter-intelligence. The authors present topics often left unexamined by professional literature, such as terminological issues, differences between various counter-intelligence concepts, and counter-intelligence dilemmas, all of which have a significant impact on national security. The examined topics and issues are not only interesting in themselves but also touch upon important social issues, *e.g.* the democratic oversight of counter-intelligence services, the question of human rights, the lawful protection of national security, the role of ethics in the system of national security, *etc*. A thorough examination of these issues will increase the general awareness of the importance of counter-intelligence, contribute to a better regulation of the field, and raise the levels of safety culture.

Despite dealing with topics relatively unknown to the public, the book is suitable for both expert and lay readership. So far European counter-intelligence has mostly looked to foreign, especially American professional literature; the present book departs from interiorized outside perspectives of the field and represents an important step in the development of the theory of counter-intelligence in the European region.

Dr. Branko Lobnikar
Faculty of Criminal Justice and Security
University of Maribor
Slovenia

PREFACE

This book presents the reader with the anatomy of European counter-intelligence, with particular emphasis on the counter-intelligence *modus vivendi et operandi* prevalent in the Balkans. Even though seemingly identical, counter-intelligence methods do in fact differ from one region to another. A subtle examination presents a complex picture, which shows that counter-intelligence methods remain strikingly consistent through time but are simultaneously shaped and affected by historical circumstances, political systems and decisions, socio-economic factors, culture, customs, and most importantly—by the people who use them. The European and Balkan counter-intelligence practices rely on *unstated* principles and *unwritten* rules. The present text, however, will say and reveal enough to show the attentive reader where the truth begins.

Dr. Iztok Podbregar
Faculty of Organizational Sciences
University of Maribor
Kranj
Slovenia

Dr. Teodora Ivanuša
Faculty of Logistics
University of Maribor
Celje
Slovenia

List of Contributors

Gašper Hribar	Department of Security, Defense and Military Logistics, University of Maribor, Mariborska cesta 7, SI-3000 Celje, Slovenia
Iztok Podbregar	Department of Organization and Management, Faculty of Organizational Sciences, University of Maribor, Kidričeva cesta 55a, SI-4000 Kranj, Slovenia
Janez Žirovnik	District Court of Maribor, Sodna ulica 14, SI-2503 Maribor, Slovenia
Teodora Ivanuša	Department of Security, Defense and Military Logistics, University of Maribor, Mariborska cesta 7, SI-3000 Celje, Slovenia

CHAPTER 1

The Anatomy of Counterintelligence: The Origins of European Perspective

Janez Žirovnik[1] and **Iztok Podbregar**[2,*]

[1] *District Court of Maribor, Sodna ulica 14, SI-2503 Maribor, Slovenia*

[2] *Department of Organization and Management, Faculty of Organizational Sciences, University of Maribor, Kidričeva cesta 55a, SI-4000 Kranj, Slovenia*

Abstract: Over the past few decades, the field of counterintelligence has become increasingly accessible to lay and professional public; this is the result of many factors, such as the opening of state archives, the declassification of secret documents, materials and literature pertaining to intelligence, counterintelligence, and security services, initiatives for improved oversight, democratization of society and political systems, human curiosity, and especially the need for a new paradigm of counterintelligence. When faced with the question of how to proceed, we encounter the following problem: there are numerous understandings, definitions, and practices of counterintelligence across the world. The European region is also pressed with the necessity of finding a new counterintelligence paradigm and often looks for answers to American literature because it is the most publicly accessible. We wish to emphasize, however, that there is a specifically European perspective on counterintelligence, which is not adequately covered in literature. There are some minor but also fundamental differences between the European and American perspectives, so that the 'general' concept of counterintelligence, which is mostly based on US literature, should also be examined form a European perspective; this is important for European and non-European countries alike. A partial European perspective on (primarily) the theory of counterintelligence is presented; it is based on the Balkans, since the regional counterintelligence was heavily influenced by other European services and thus reflects a European counterintelligence viewpoint. At the same time, the Balkan states possess a more complex view of counterintelligence, which is not well known in the world.

[*] **Corresponding author Iztok Podbregar:** Department of Organization and Management, Faculty of Organizational Sciences, University of Maribor, Kidričeva cesta 55a, SI-4000 Kranj, Slovenia; Tel: + 386 (0)4 23 74 291; Fax: +386 4 23 74 299; E-mail: iztok.podbregar@fov.uni-mb.si

Iztok Podbregar & Teodora Ivanuša (Eds.)

Keywords: Balkans, Communication interception, Counterintelligence, German national intelligence and security system, Intelligence, Intelligence and security service, Literature on counterintelligence.

INTRODUCTION

As a rule, the general public is not familiar with the nature of counterintelligence due to its specific, *i.e.* the need to protect national security and interests and to ensure the safety of methods, sources, capacities, means, organization, and the intelligence and security services personnel. The past few decades have seen an increase in the available literature on counterintelligence activities. This has resulted in the gradual unveiling of counterintelligence secrets and contributed to the debunking and breaking of some related stereotypes and taboos.

Within the context of intelligence and security, counterintelligence offers a safe framework for the realization of umbrella activities: it provides protection from foreign secret agents and operatives, from misleading information, disclosure of classified information, harmful foreign interests, *etc*. In cases where this protection is either non-existent or compromised, the functioning of the entire intelligence and security service or the national security system is directly or indirectly threatened. The term counterintelligence includes intelligence activities, counterintelligence activities, and their combinations. The relevant Slovene scientific terminology (*e.g.* Purg, 1995; Anžič, 1997; Šaponja, 1999; Miklavčič, 2001; Podbregar, 2008, 2012; Henigman, 2008; Čaleta, 2009; Rode, 2010; Sotlar, 2012; Koren, 2012) uses the joint expression intelligence and security (in Slovene: obveščevalno-varnostna dejavnost), which can be separated into three branches (Podbregar, 2008): intelligence, counterintelligence, and security. The classification prevalent in some Balkan states thus sees it as a given that intelligence includes counterintelligence; it thus differs from the accepted American terminology. However, we propose that the branch of counterintelligence is not necessarily dialectical to or interdependent (one could even say synergic) with the intelligence branch; the two of them are not always identical. We could therefore reasonably expect Slovene terminology to apply the following term: intelligence, counterintelligence, and security.

The intelligence and security training run by intelligence and security services is not open to public, which is why its contents remain relatively unknown. However, this is not the case with training organized by public and private institutions. These equip their students with the basics of intelligence and security and the relevant methods (especially legal methods, such as collecting intelligence from open sources, *i.e.* OSINT) and acquaint them with the literature available to the general public or the interested public (researchers, academic, journalists, historians, citizens). The most important 'public' providers of such courses are educational institutions, particularly higher education institutions. It seems, however, that the majority of graduates are unable or incapable of fully applying the acquired knowledge in their everyday lives, *e.g.* at work, in research, or as part of systems thinking, and only few continue to become part of intelligence and security services; for the most part their basic knowledge is transferred to a new institution, where it is upgraded and practically applied.

Anthony Glees argues that universities, *i.e.* tertiary institutions, should focus more attention on intelligence, specifically by introducing relevant intelligence content into their curricula. This would enhance public understanding of intelligence matters; on the other hand, the public's familiarity with examples of good and bad practice would lead to improvements in intelligence practice. Glees emphasizes that study programs should be amended in a way that students are no longer primarily trained to be specialists (for example, in analytical work) but are instead educated to become generalists with an in-depth knowledge of the entirety of the intelligence process. This would enable the students to provide a detached, critical assessment of the process; such rigorous academic training would later serve to enhance the quality of the field of intelligence (Glees, 2015).

The risks of over-specialization were eloquently discussed by Ludwig von Bertalanffy, the author of the General System Theory (1968), who realized that the students of systems sciences lack a general overview of their area; at the same time they were over-specialized in technical knowledge. Bertalanffy took this to be an example of the principle of modern mechanization, where the individual is a mere cog in the social machine and is thus reduced to a role of a highly- but also narrowly-trained, mindless button-pushing specialist (the original refers to this type of person as a moron or a learned idiot). The system as a whole, on the other

CHAPTER 2

The Foundations of Counterintelligence: Definition and Principles

Gašper Hribar*

Department of Security, Defense and Military Logistics, University of Maribor, Mariborska cesta 7, SI-3000 Celje, Slovenia

Abstract: The comparative analysis of American and European literature has revealed the main reasons for the differences in the understanding of counterintelligence; these are the result of varieties in linguistic use, the different interpretations of the expression counterintelligence, and the grouping of various activities under a single umbrella activity and service due to similar methods of work, identical or common threats, and similar goals. The wealth of available literature demonstrates that counterintelligence has been given increasing research attention; however, there is no consensus regarding the definition of counterintelligence. This is further reflected in practice, which then feeds back into the theoretical development of counterintelligence. To remedy this, we propose a new definition of counterintelligence, which was shaped on the basis of analyzed literature and therefore stems from theory rather than practice. On the basis of definition, we have come up with two representations: 1) representation of the counterintelligence process; 2) representation of the counterintelligence process operating against foreign intelligence activity. These two representations illustrate the working of counterintelligence and counterintelligence services in practice; they are based on the proposed definition and the idea that counterintelligence is aimed at foreign intelligence activity and processes but not at foreign security and other security threats, which are not the result of intelligence activities. The chapter concludes with the description of some unwritten counterintelligence principles, which are part of counterintelligence subculture.

* **Corresponding author Gašper Hribar:** Department of Security, Defense and Military Logistics, University of Maribor, Mariborska cesta 7, SI-3000 Celje, Slovenia; Tel: +386 3 428 53 67; Fax: +386 3 428 53 38; E-mail: gasper.hribar1@um.si

Keywords: Counter-espionage, Counterintelligence process, Counterintelligence service, Definition of counterintelligence, Principles of counterintelligence, Security service.

INTRODUCTION

Counterintelligence is known and employed globally and therefore not limited to particular areas of the world. The same can be said of security and defense and their elements: their principles and foundations are alike across the world, while certain aspects may differ from one country to another because of their adaptation to specific social and natural environments. It would be, therefore, natural to assume that perceptions of counterintelligence would also be comparable, as well as views of its 'sister' activity, intelligence. A survey of scientific and professional literature in the field shows that counterintelligence is thoroughly researched, with some variety existing in the numerous definitions of the field. As we shall see later, the definitions in American literature differ from those in the European literature. Similarly, there are differences in terms of the mission, functioning, and functions of specific US and European counterintelligence and security services; despite the services pursuing similar (or even identical) activities, they are designated by different functional names (*e.g.* security service, domestic intelligence agency, counterintelligence service), they do not have the same competences, they have dissimilar tasks, different powers, *etc*. Such variance may be the result of numerous complex causes, among them differences in political systems, legal systems, the role and notion of human rights and freedoms, nation and state history (both on macro and micro levels), culture and mentalities, economy and industry, state interests, geostrategic position of the country, and so on. However, at least the basics of counterintelligence should be understood identically. The American definitions of counterintelligence are somewhat wider than European and also include counter-espionage, counter-terrorism, counter-sabotage, safeguarding of classified information, issues related to WMD, *etc*. In Europe, counterintelligence is defined in a narrower sense, as the 'antagonism' between two or more intelligence subjects (for example, intelligence services) with the intention of the prevention of foreign espionage by various possible means.

TERMINOLOGICAL ISSUES IN THE DEFINITION OF COUNTERINTELLIGENCE

As suggested by the name itself, counterintelligence activities are aimed against (foreign) intelligence. Our starting point is the English term counterintelligence (also spelled counter intelligence or counter-intelligence), which is comprised of two words: counter (to be or act against, to oppose someone or something) and intelligence. Despite the ostensible simplicity of the meaning, there is no uniform understanding of its scope. The more populist versions equate counterintelligence with counter-espionage and in some places also with counter-terrorism. Academic and professional accounts variously define counterintelligence as a separate discipline in the intelligence process, as an activity complementary to intelligence, or counterintelligence as part of security. These differences in understanding are also present on the national level, as evident, for example, when looking at the American and European (especially continental) views of counterintelligence, and also globally. These variations are furthermore mirrored in the various practices of counterintelligence across the world, which differ widely in their functions and jurisdictions, with some services having the powers to arrest and use various investigative measures on domestic territory (for example, the American FBI, the Russian FSB, the Serbian BIA, and Israeli Shin Bet), and others without such competences (for example, the Slovene SOVA, the German BfV, the English MI5, the Australian ASIO, the Canadian CSIS).

These discrepancies can most commonly be attributed to the following factors:

- Language, *i.e.* varieties in linguistic use and meaning in various languages;
- Different interpretations of the term ‘intelligence’;
- The equating or grouping of several different activities into a single umbrella activity due to similar methods of work, identical or similar threats, and comparable goals;
- Different political structures and political systems, which affect the organization of intelligence and security;
- Rivalry and competition in the professional and academic spheres;
- Different views and interpretations on the part of professionals, theoreticians, academics, journalists, and researchers.

CHAPTER 3

Some Counterintelligence Methods

Teodora Ivanuša*

Department of Security and Defense & Military Logistics, Faculty of Logistics, University of Maribor, Mariborska cesta 7, SI-3000 Celje, Slovenia

Abstract: Even though the greater part of intelligence has moved into virtual space, this is not the case with counterintelligence: its essential, core part still remains moored in the real world. Modern technology cannot replace people, especially not in counterintelligence, which is why fundamental counterintelligence methods are rooted in people and human activity. Today's counterintelligence methods and methodics are similar and even identical to those from the past, except that they have adapted to technological advances and societal changes; the methodology of counterintelligence, however, remains unchanged. Some fundamental counterintelligence methods are examined, which have not significantly changed through history—we are referring to the use of double combination and the process of handling double agents, moles, defectors, covert surveillance of people, things, and facilities, denial, deception, counterintelligence protection, counter-surveillance, counter-denial, and counter-deception.

Keywords: Counter-deception, Counter-denial, Counter-surveillance, Counter-intelligence methods, Counterintelligence protection, Covert surveillance, Deception, Defector, Denial, Double agent, Double combination, Mole.

INTRODUCTION

Before turning our attention to counterintelligence methods, we should differentiate between the terms method, methodics, and methodology; the difference between them was aptly described by Matjaž Mulej (in Ivanuša, 2013,

* **Corresponding author Teodora Ivanuša:** Department of Security and Defense & Military Logistics, Faculty of Logistics, University of Maribor, Mariborska cesta 7, SI-3000 Celje, Slovenia; Tel: +386 3 428 53 67; Fax: +386 3 428 53 38; E-mail: teodora.ivanusa@um.si

pp. 105-106), the author of the *Dialectic Systems Theory*:

> Methodology is the study of methods, which also includes the creation and application of new methods. Methodics is the study of given methods, which does not entail the creation of new methods. Methods refer to practice. Consequently, methods appear as operative work procedures. Teachers, for instance, are thus taught methodics for teaching Slovene, Math, and so on, *i.e.* they are taught descriptions of methods and the instructions for their standardized use, with little space for creativity. Methodologies refer to theoretical foundations. Each of the three, method, methodics, or methodology, may either modify or maintain the same characteristics.

Following Mulej's explication, a method is a praxis which realizes or materializes the intended theoretical foundations (methodologies) in accordance with specific rules, instructions, or guidelines (methodics); the rules, guidelines, and instructions themselves stem from methodology. Counterintelligence activities need to be based on correct and appropriate theoretical foundations, since these are the ground of normative structures and practices.

A comparison of contemporary and historical methods (Hribar, 2013) has shown that today's counterintelligence methods and methodics do not differ significantly from the ones used throughout history; this indicates that counterintelligence methodology has not significantly altered. The only evidence of change is to be found in methods which have to a certain degree adapted to technological progress and societal change, especially to legislature and the (democratic) oversight of services (ibid.). Nowadays, the majority of intelligence processes and 'conflicts' take place in virtual space, which is therefore also the scene of counterintelligence and intelligence support. Despite technological advances that have partially or entirely replaced humans in certain areas of life and the transfer of a considerable amount of activities from real into virtual environments, the counterintelligence 'core' remains firmly moored in real space, *i.e.* the domain of people.

There are numerous classifications of counterintelligence methods in the available literature. The American authors, in particular, tend to refer to measures rather than methods, whereas others use terms such as operations, techniques, and so on. Correspondingly, there is a variety of available categorizations and descriptions of counterintelligence methods, for instance, methods of exploitation, methods of neutralization, and offensive methods (United States Marine Corps, 1998); offensive and defensive operations and data collection operations (Lowenthal, 2014); support apparatus, interrogation, (physical) surveillance and technical double agents, penetration agents (moles), defectors, alliances and document merging (Johnson, 2009); tools in Behavioral Tools and Techniques: detection of manipulation and prediction methods (Pool, 2010); prevention of enemy penetration, protection from unauthorized leaks of confidential data, prevention of espionage, subversion, sabotage, terrorism, and other politically motivated actions, and the prevention of theft of key technology and equipment (Kuloğlu, Gül & Erçetin, 2014). On the basis of analyzed literature, methods can be separated according to their characteristics into offensive methods and defensive methods.

Offensive methods are all methods actively employed by the counterintelligence service against the enemy with the intent to detect, harm, weaken, or destroy the enemy, to acquire specific information, equipment, or objects, to deceive or plant their own information or people (double agent, mole) tasked with transmission of data or with influencing decisions. The above mentioned methods are based on three major activities: detection, manipulation, and neutralization (Kuloğlu, Gül & Erçetin, 2014). Offensive counterintelligence activities are predicated on establishing contact with specific (confidential) information or person, or, in other words, on spotting, defining, and engaging the target (goal) which is the subject of the offensive activities. Unless the target is known, the service cannot apply offensive methods, since this would equal shooting randomly in the forest, hoping to catch one of the animals we cannot see. Offensive methods benefit the counterintelligence service while simultaneously directly or indirectly harm the foreign intelligence service.

Defensive methods are methods actively and passively employed against the adversary working against us. These methods are used for prevention, entrapment,

CHAPTER 4

Counterintelligence Operatives, Targets, Foreign Agents and Foreign Operatives

Teodora Ivanuša[1] and **Iztok Podbregar**[2,*]

[1] *Department of Security, Defense and Military Logistics, University of Maribor, Mariborska cesta 7, SI-3000 Celje, Slovenia*

[2] *Department of Organization and Management, Faculty of Organizational Sciences, University of Maribor, Kidričeva cesta 55a, SI-4000 Kranj, Slovenia*

Abstract: The chapter is dedicated to human resources in the field of counterintelligence. Whereas, technological developments have brought about progress in intelligence, counterintelligence, and security, the human element has remained unchanged since the very beginning and remains key part of counterintelligence. The section presents some of the main characteristics of counterintelligence operatives, especially in relation to what shaped them and why. It is important to fully understand these circumstances and reasons, since anyone can, knowingly or unknowingly, become the target of foreign intelligence activity, *e.g.* a secret agent, an intermediary, or bait; the text looks at factors that influence whether a person is of interest to a foreign service. People of interest to foreign services often become secret agents, which is why it is important for counterintelligence services to be aware of the indicators that may alert them to foreign agents and to be familiar with the most common groups of people recruited as secret agents. Such knowledge should also be vital to state officials as well as people in the industry (especially in high tech, energetics, tele-communications, *etc.*), since it can contribute to a timely detection of spies. Operatives are trained in concealing their identities and covering their tracks, so they are more difficult to uncover than agents. A special form of operative is discussed, *i.e.* an operative working under the guise of a diplomat.

* **Corresponding author Iztok Podbregar:** Department of Organization and Management, Faculty of Organizational Sciences, University of Maribor, Kidričeva cesta 55a, SI-4000 Kranj, Slovenia; Tel: +386 4 23 74 291; Fax: +386 4 23 74 299; E-mail: iztok.podbregar@fov.uni-mb.si

Iztok Podbregar & Teodora Ivanuša (Eds.)

Keywords: Counterintelligence personnel, Diplomats, Espionage, Foreign agents, Foreign operatives, Indicators, Motives, Secret agents, Targets.

INTRODUCTION

The human individual is the central element of counterintelligence. This chapter is devoted to counterintelligence human resources and will look at various profiles found in the field: the characteristics of counterintelligence operatives, foreign intelligence targets, agents or secret agents and indicators that alert us to their presence, and foreign operatives.

COUNTERINTELLIGENCE PERSONNEL

The stereotypical image of a counterintelligence operative is that of a skeptic who finds it difficult to trust others and sees potential enemies everywhere, even among their own rank. Of course, some of these clichés are undoubtedly founded on specific character traits and behavior affected by the nature of their work. It is understandable that no-one wishes to be controlled, all the more so in contemporary society, where—because of globalization, IT, and political liberalization—individuals are far better aware of their rights and duties and limitations of others, especially when it comes to privacy; they are thus pre-disposed to revolt against control. This type of revolt can be found in all services which carry out (internal) oversight of staff and their work, *e.g.* in military organizations, security and police organizations, other services with public authorization, organizational units, public institutions, *etc*. The so-called internal affairs or services for internal oversight are generally not held in high esteem by their colleagues, which is why the staff tries to avoid them whenever possible. Due to the specifics of counterintelligence work, counterintelligence control is somewhat different from other types of control. Most services conduct internal controls on the basis of a tip-off or perceived anomalies (following the course of duty); counterintelligence control, however, does not need to be instituted on the grounds of a report or specific (official) grounds. Counterintelligence also significantly differs in terms of the effects of the final results of the control: in most organizations these are generally presented to other people (*e.g.* to the person being investigated and their superiors) or bodies (*e.g.* disciplinary and

inspection bodies, prosecuting authorities); in counterintelligence, however, the results are generally not shared, especially not with the person under investigation. In some cases, the results of counterintelligence control remain the internal affair of the service or organizational unit and the person investigated never finds out they were subject of control. Counterintelligence personnel is more likely to accept internal control when it is entrusted to experienced operatives and/or respected members of the organization with great integrity, a comprehensive knowledge of counterintelligence, and a wide perspective of the field and the service. The choice of investigative staff decisively affects trust.

As already mentioned, counterintelligence stereotypes are the result of the operatives' roles and their behavior. Being a counterintelligence operative is emotionally and intellectually challenging. Operatives should be exceptionally patient, consistent, and cautious, and often exhibit those same characteristics in their personal lives. Just as with intelligence operatives, their schedules are merciless: they are always at work, regardless of the time (every second, every day of the year, during holidays), place (at home, place of work, or elsewhere), or circumstances (family matters, work matters, or personal matters). They can always end up being the target of foreign intelligence or counterintelligence, which is why they need to be constantly alert to their surroundings and act cautiously and inconspicuously. Over time the initial feelings of distrust may grow into a permanent state of mind that has made counterintelligence operatives known for their inability to trust.

It is important for counterintelligence operatives to be good analysts with a rich knowledge and experience in operative work; they need to be familiar with intelligence and counterintelligence method of both domestic and foreign services and need to have specific knowledge in the fields of psychology, sociology, history, *etc*. Because of the always present possibility of enemy deception, operatives should treat work material consistently, cautiously, and with a certain measure of distrust. All of this breeds skepticism or doubt in everything that the operative handles, perceives, or believes to exist; the end results are never fully reliable or trustworthy. It is therefore imperative that the operative be grounded and rational, but also highly imaginative, since this allows them to look for possible solutions or explanations. The operative should also be capable of

CHAPTER 5

Some Counterintelligence Dilemmas

Iztok Podbregar*

Department of Organization and Management, Faculty of Organizational Sciences, University of Maribor, Kidričeva cesta 55a, SI-4000 Kranj, Slovenia

Abstract: The chapter presents contemporary issues worthy of more detailed attention in theory and especially in practice of counterintelligence. The first dilemma concerns the question of ethics in counterintelligence, which has long been a source of contention among lawyers, sociologists, philosophers, and practicians in the field of security. The text furthermore highlights the problem of 'grey zone' in counter-intelligence and explains why ethical counterintelligence is an oxymoron; it confronts the reader with the ethical dilemma of the relative importance of national security *vs.* individual's human rights. A slightly less known modern issue is the question of OSINT and its legality; foreign intelligence services can use OSINT to extend from ostensibly legal into half-legal or illegal fields of activity and thus avoid counterintelligence surveillance and the activities of other services. The last issue presented is the question of trust among partner state services; in 2015 we witnessed the disclosure of documents revealing the extent of NSA surveillance of leaders, ministers, and state body officials from Germany, France, Brazil and Japan. These revelations sparked a debate on the acceptability of spying on 'friendly' or partner states; in itself this is not a new dilemma, however it was previously unknown to the public.

Keywords: Disinformation, Eavesdropping, Ethics, Exploitation, Friendly intelligence, Grey zone, Manipulation, National security, NSA, OSINT, Oxymoron, Semi-legal, Torture, Trust, WikiLeaks.

* **Corresponding author Iztok Podbregar:** Department of Organization and Management, Faculty of Organizational Sciences, University of Maribor, Kidričeva cesta 55a, SI-4000 Kranj, Slovenia; Tel: +386 4 23 74 291; Fax: +386 4 23 74 299; E-mail: iztok.podbregar@fov.uni-mb.si

INTRODUCTION

Even though counterintelligence is a vital and indispensable element or building block of the system of national security (Kuloğlu, Gül & Erçetin, 2014), certain segments of the field remain ambiguous, open, and problematic. These issues or dilemmas directly or indirectly affect the field of counterintelligence. This chapter will present some of these dilemmas which demand greater attention, in practice as well as in theory, especially due to factors such as the environment, time, and the level of societal progress.

COUNTERINTELLIGENCE AND ETHICS

Ethics in the field of counterintelligence may be approached from two different standpoints: the individual perspective, *i.e.* the ethics of people working in counterintelligence, and the perspective of the ethics of the methods involved. It is reasonable to expect for ethics to apply equally to all individuals in counterintelligence, which is why in this case ethics will be discussed generally; when it comes to ethics related to methods, the specificities of counterintelligence field demand us to focus exclusively on the ethics of counterintelligence methods.

Operational ethics in intelligence, counterintelligence, and security can be treated conjointly, since all of the employees should operate ethically, regardless of their surroundings, circumstances, personal characteristics, desires, and the work they are doing. Intelligence, counterintelligence, and security work differs significantly from other areas of action, which is why it is guided by a special set of rules and principles. Legality, secrecy, safety culture, organizational loyalty, patriotism and integrity (Pleteršek, 2008) are just some of the principles binding the employees in the above fields to ethically and morally acceptable and appropriate behavior. It is vital that the personnel act ethically, since this prevents negative occurrences with potentially harmful consequences, especially in the field of counter-intelligence, *e.g.* the penetration of the service by a foreign force (due to negligence, contentious or unlawful activities, corruption, dependencies), defection, (high) treason, and other threats. Ethically guided functioning is thus an important part of the safety culture and the accompanying counterintelligence protection. Counterintelligence and security ethics are important because of the

contemporary challenges the services encounter in their work: the shifting roles of intelligence, counterintelligence, and security services, the increasing demand for the respect and observance of human rights, and the past errors, affairs, and controversies related to Western services and concerns voiced by the international communities in relation to these negative events (Born & Wills, 2010, p. 35). The available literature (*e.g.* Gendron, 2005; Quinlan, 2007; Shapiro, 2007; Gill, 2009; Omand & Phythian, 2013) presents numerous perspectives on the ethics of intelligence and security, which differ on philosophical, sociological, cultural, and professional grounds. Loosely speaking, there are those theories that argue that the end justifies the means, others that give primacy to human rights, and those trying to build a bridge between the extremes of the first two groups; there is thus no consensus as to what constitutes ethics in intelligence and security. In terms of methods, we will not be discussing the issues of abuse of position or jurisdiction and thus the misuse of counterintelligence methods for illegal and private goals; instead, we will focus on the discussion of the 'nature' of counterintelligence methods from the standpoint of ethics.

In order to do so, we first need to remind the reader that counterintelligence is a complex field dominated by ambiguous, fuzzy threats, risks, dangers and related circumstances. Apart from ambiguous factors appearing as the result of foreign service activity, there is also the possibility of asymmetry, *i.e.* a situation in which the foreign service holds considerable advantage over the counterintelligence service (and *vice versa*). The effective deterrence, prevention, countering, or exploitation of foreign intelligence activities thus calls for an alternative approach that differs considerably from more customary approaches: our ways of thinking should be adapted appropriately. It would be unreasonable to demand that counterintelligence services fight foreign intelligence activity (be it ethical or unethical) with ethical means only—this would severely circumscribe the effectiveness of their response. It is no secret that counterintelligence, intelligence, and security fields employ a wide range of methods, apart from legal and illegal also methods found in the so-called grey zone. The grey zone is a space of transition, where legitimate and legal methods pass into illegitimate and illegal methods, but are neither specifically allowed nor specifically forbidden. The ethics and morality of these methods are questionable; at the same time, they

CHAPTER 6

Brigadier General Vladimir Vauhnik: Famous Slovenian/Yugoslav Operative

Teodora Ivanuša*

Department of Security, Defense and Military Logistics, Faculty of Logistics, University of Maribor, Mariborska cesta 7, SI-3000 Celje, Slovenia

Abstract: Vladimir Vauhnik, first colonel and then brigadier general in the army of Kingdom of Yugoslavia, is an important and yet almost forgotten figure of the Second World War; his efforts might have changed the course of the war for the better. Prior to and during the Second World War, Vauhnik was Yugoslavia's military attaché to Berlin, where he spied on Germans. He used covert and legal methods to obtain information on the basis of which he was probably the first in the world to determine that Nazi Germany would invade Poland, and later, the Kingdom of Yugoslavia and the Soviet Union. The chapter presents a section from Vauhnik's autobiography, in particular the difficulties caused by Vauhnik's intelligence and counterintelligence activities to the German counterintelligence and the Gestapo, which was run by Vauhnik's 'nemesis', Walter Schellenberg. Vauhnik was successful in evading the Germans, but was eventually put under surveillance and then arrested together with other Yugoslav intelligence operatives in Germany and occupied territories, following Hitler's orders.

Keywords: Berlin, Counterintelligence, Diplomacy, Espionage, Gesellschaftsspionage, Gestapo, Invasion of Yugoslavia, Kingdom of Yugoslavia, Military attaché, Military intelligence, Nazi Germany, Vladimir Vauhnik, Walter Schellenberg.

* **Corresponding author Teodora Ivanuša:** Department of Security, Defense and Military Logistics, University of Maribor, Mariborska cesta 7, SI-3000 Celje, Slovenia; Tel: +386 3 428 53 67; Fax: +386 3 428 53 38; E-mail: teodora.ivanusa@um.si

INTRODUCTION

General Vladimir Vauhnik was one of the most famous European spies in the period before and during the Second World War who deserves special attention for his intelligence and counterintelligence successes.

VLADIMIR VAUHNIK: A SHORT BIOGRAPHY

Vladimir Vauhnik was born on the 24th June 1896 in Svetinje near Ormož in Slovenia. He graduated at the Classical Gymnasium in Maribor, where he excelled in Maths. He continued his studies in the cadet school in Maribor and later at the military academy Theresianum in Austria, the higher military school and the general staff academy in Belgrade, and the French military school in Saint-Cyr. The Yugoslav General Staff sent him to complete his training in the French and English General Staff. He spoke several European languages and served as a university professor of strategy and tactics. In 1937, he was named the military attaché to Berlin—at the time he was a colonel (in 1944 Draža Mihajlović promoted him to brigadier general). When Nazi Germany attacked the Kingdom of Yugoslavia in 1941, the Gestapo arrested him and detained him for four months. After his arrest, Vauhnik returned to Ljubljana and organized the ally intelligence service. When the service was discovered, he was forced to escape to Switzerland; in 1947 he emigrated to Buenos Aires, where he died on 31st March in 1955. Vauhnik's remains were later moved to Slovenia, to his family tomb in Slovenske Gorice.

VAUHNIK AS AN OPERATIVE IN NAZI GERMANY

Vauhnik was known as an excellent intelligence and counterintelligence operative and analyst. His genius for obtaining information was most apparent during his time serving as an attaché in Berlin. He used various methods for collecting information (some of them quite legal) and used them to predict occurrences that no-one else was able to at the time. He is especially known for being probably the first person in the world to get information on planned Nazi attacks on Poland, the Kingdom of Yugoslavia, and the Soviet Union.

Vauhnik was a thorn in the side of the German counterintelligence or the Gestapo,

since he was intelligent, careful, and cunning. Even though he collected a considerable amount of intelligence, he was never caught by the counterintelligence; his greatest adversary was Walter Schellenberg who "(…) was the head of the entire German secret police. After Admiral Canaris' execution, whom Schellenberg arrested personally following a court order, Schellenberg also took over the intelligence service of the German army, which had been led by Canaris; the entire intelligence service of the Third Reich was thus concentrated in his hands. Schellenberg was one of the German officials convicted in the Nuremberg trials. When he was freed, he moved to Italy and lived there until his death. He wrote a memoir that came out in German and English, in which one of the chapters was devoted to Colonel Vauhnik", (Vauhnik, 1965, p. 421). The memoir came out in English in 1956 (The Schellenberg Memoir) and then in German in 1959 (Walter Schellenberg Memoiren).

In his memoirs Schellenberg (Hafner in Vauhnik, 1965, pp.425-427) "writes about his rise to the highest position in German espionage, the circumstances of some members of the high society, and also about various adventures and exploits in espionage. He tells incredible stories that played out behind the scenes and describes the activities of German espionage and their fight with enemy groups and individuals. In the entire memoir, which is 356 pages long, he devotes only one chapter to a single adversary, an adversary he could never defeat throughout the time that Yugoslavia was a country, even though he was serving in Berlin as a Yugoslav military attaché—Colonel Vladimir Vauhnik".

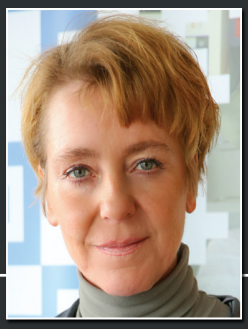
The chapter on his antagonism to Vauhnik "is entitled "Gesellschaftsspionage" (social espionage) (…) Schellenberg touches on the period between 1940 to 1941. Let us look at Schellenberg's own account of how Vauhnik related to Belgrade ahead of time that the capital by the Danube will be bombed. 'For several months we have received regular reports about all the secret reports coming from Yugoslav foreign missions. Among them, reports by the Yugoslav military attaché to Berlin, Colonel V., attracted special attention. The transcripts of the reports were sent to us directly by one of our agents in the Belgrade ministry of foreign affairs. The military attaché's reports exhibited such a vast and detailed knowledge of our military and political plans that we were repeatedly left

AUTHOR INDEX

SUBJECT INDEX

IZTOK PODBREGAR

Dr. Iztok Podbregar is a Professor of Leadership and Management in Security Organizations. He held numerous positions in the Slovenian national security system: the head of the Air Force Department in Slovenian Armed Forces (1991-1994), the Deputy Chief of Defense (1995-1998) and a Chief of Defense (1998-2001) of the Republic of Slovenia, the State Secretary at the Ministry of Defense, a Senior Advisor of the Prime Minister of the Republic of Slovenia (2001-2002), the Director of the Slovenian Intelligence and Security Agency (2002- 2006), the National Coordinator for the Fight Against Terrorism (2004-2006), and a Senior Advisor to the President of the Republic of Slovenia (2006-2007). Dr. Podbregar teaches at different faculties of the University of Maribor (the Faculty of Organizational Sciences, the Faculty of Criminal Justice and Security, the Faculty of Logistics, and the Faculty of Tourism). Since 2016, he has been serving as the Dean of the Faculty of Organizational Sciences, University of Maribor.



TEODORA IVANUŠA

Dr. Teodora Ivanuša is an associate Professor and the head of the Department of Defense and Military Logistics at the Faculty of Logistics, University of Maribor, where she conducts lectures on the subjects of terrorism and weapons of mass destruction, security, defense and military, and systems theory. She attained PhD degree in Diagnostic Imaging and in System Theory. She is a former OF-5 Military Specialist, former representative in NATO/CNAD/AC225/JCGBRN, and a former Advisor for Education and Special Tasks in the Slovenian Armed Forces. During the period 2012-2015, DDr. Ivanuša also served as a member of NATO Science for Peace and Security Programme's Independent Scientific Evaluation Group (ISEG). In 2014, she was appointed as a representative of the Rector's Conference of the Republic of Slovenia to the Council of the Government of the Republic of Slovenia for protection against natural and other disasters.