



UNIVERSITATEA BABES-BOLYAI
BABES-BOLYAI TUDOMÁNYEGYETEM
BABES-BOLYAI UNIVERSITÄT
BABES-BOLYAI UNIVERSITY
TRADITIO ET EXCELLENTIA



FACULTATEA DE
ISTORIE ȘI FILOSOFIE



ȘCOALA DOCTORALĂ DE
**Relații Internaționale și
Studii de Securitate**

**“Babeș-Bolyai” University of Cluj-Napoca
Faculty of History and Philosophy
Doctoral School of International Relations and Security Studies**

**PhD Thesis
Summary**

SCIENTIFIC COORDINATOR:

Prof. Univ. Dr. Ivan Adrian Liviu

PHD STUDENT:

CLAUDIA-ALECSANDRA GABRIAN

**CLUJ-NAPOCA
2026**



UNIVERSITATEA BABEȘ-BOLYAI
BABEȘ-BOLYAI TUDOMÁNYEGYETEM
BABEȘ-BOLYAI UNIVERSITÄT
BABEȘ-BOLYAI UNIVERSITY
TRADITIO ET EXCELLENTIA



FACULTATEA DE
ISTORIE ȘI FILOSOFIE



ȘCOALA DOCTORALĂ DE
**Relații Internaționale și
Studii de Securitate**

**“Babeș-Bolyai” University of Cluj-Napoca
Faculty of History and Philosophy
Doctoral School of International Relations and Security Studies**

**THE GEOPOLITICS OF CYBERCRIME AND THE RESHAPING OF THE
CYBERCRIMINAL ECOSYSTEM SINCE THE BEGINNING OF THE RUSSO-
UKRAINIAN WAR**

**Doctoral field:
International Relations and European Studies**

SCIENTIFIC COORDINATOR:

Prof. Univ. Dr. Ivan Adrian Liviu

PHD STUDENT:

CLAUDIA-ALECSANDRA GABRIAN

**CLUJ-NAPOCA
2026**

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

CHAPTER I. THEORETICAL AND CONCEPTUAL FOUNDATIONS: THE GEOPOLITICS OF CYBERSPACE

1.1. The International Relations approach to analyzing cyberspace

1.1.1. From global interconnection to the instrumentalization of interdependence

1.1.2. Structural realism and international anarchy

1.1.3. Overcoming geographical constraints and maximizing relative power

1.2. Cyber-geopolitics theory and the security dilemma in the digital space

1.2.1. Cyberspace as a domain of conflict

1.2.2. The security dilemma in the digital age and the structural advantage of the offensive

1.2.3. Limitations of International Relations theories in analyzing cyberspace: From Neorealism to Chaos Theory

1.3. Conceptual delimitations and operationalization

1.3.1. Reconceptualizing "cybercrime": From financial offense to act of hybrid warfare

1.3.2. Typology of cybercriminals in contemporary cyberspace

1.3.3. The social contract and the psychological profile of the cybercriminal

1.4. The Russian Federation's doctrine: Cyber sovereignty and the militarization of the information space

1.4.1. The Concept of Cyber-Sovereignty and RuNet

1.5. Cyberspace as an emerging domain of strategic competition and its impact on national security

1.5.1. Typology of cyberattacks in the context of hybrid warfare

1.5.2. Definition and emergence of ransomware attacks

CHAPTER II. THE CYBERCRIME ECOSYSTEM IN THE RUSSIAN FEDERATION: THE CONVERGENCE OF PROFIT AND STRATEGIC OBJECTIVES

2.1. The Russian Federation's security paradigm and digital sovereignty

2.1.1. From legal protection to instrumentalization: recruitment mechanisms in cyberspace

2.1.2. Selective enforcement as a mechanism for co-optation and the management of cyber resources

2.2. The financial infrastructure of the criminal ecosystem: exploitation of IABS systems, cryptocurrencies, and money laundering mechanisms

2.2.1. The cryptocurrency ecosystem

2.2.2. Operational infrastructure on the Dark Web

2.2.3. The "underground" ecosystem and Dark Web forums

2.2.4. Initial Access Brokers and their role in the cybercrime ecosystem

2.3. Dynamics of the criminal ecosystem in the context of the February 24, 2022 invasion

2.3.1. Shifting Target Selection

2.3.2. Efficiency and Vulnerabilities of the Proxy Model

2.4. Automating the Offensive: Integrating Artificial Intelligence into the Ransomware Ecosystem

2.4.1. Transition to Next-Generation Warfare on the European Flank

2.4.2. Strategic Information Attack Doctrine: From Psychological Subversion to Technical Blockade

CHAPTER III. COMPARATIVE ANALYSIS OF THE RANSOMWARE ECOSYSTEM: THE CONTI AND BLACK BASTA CASES

3.1. Operational Continuity of Ransomware Groups

3.2. The Conti Ransomware Group

3.2.1. Conti Leaks

3.3. The Black Basta Ransomware Group

3.3.1. Black Basta Leaks

CHAPTER IV. THE RANSOMWARE ECOSYSTEM AND ITS EVOLUTION

4.1. Analysis of the Ransomware Ecosystem in 2025

4.2. Ransomware Evolution in 2026 and Future Outlook

4.2.1. Ransomware Leaks in 2026

4.3. Cyber-Intelligence: An Essential Tool for Enhancing National Security in the Digital Age

4.4. The Role of International Institutions in Combating Cybercrime

CONCLUSIONS

BIBLIOGRAPHY

Keywords: ransomware, cybercrime, geopolitics, hybrid warfare, dark web, Telegram, IABS, Conti, Black Basta, The Gentlemen

INTRODUCTION

At present, cyberspace is no longer limited to a global communications network or an environment intended exclusively for businesses and technological innovation. Within the contemporary architecture of international relations, it represents one of the most active, volatile, and difficult-to-control domains, having gradually become an arena of geopolitical competition among major powers. This transformation has been made possible by the decentralised nature of the Internet, which has diminished the significance of geographical boundaries in the conduct of activities in cyberspace. Cybercriminals are among the principal actors in the digital environment who have contributed to the reconfiguration of the balance of power, with decentralisation representing a significant advantage for them.

These cybercriminals may be organised into large or small groups of individuals possessing technical expertise and advanced computing capabilities. Their capacity to exert influence within the global security environment may be comparable to that exercised by a state. Since 2022, cyberspace has become an increasingly dynamic and unpredictable environment, while transnational cybercrime has evolved beyond the scope of conventional approaches to addressing criminal activity. Data theft and extortion no longer constitute exclusively financial crimes; they have also become matters of national security and instruments for exerting asymmetric influence in the competition among state actors.

The evolution of cyber threats marks a paradigm shift in the conduct of international conflicts. For example, in previous decades, a significant proportion of cyberattacks were carried out by individuals or small groups motivated by curiosity or the pursuit of occasional financial gains. Today, the cyber landscape is characterised by the emergence of specialised ransomware criminal organisations that are no longer driven solely by financial motives and rely on extensive affiliate networks.

Ransomware groups are complex organisational structures with substantial financial resources, specialised operational functions, and clearly defined hierarchical levels. Over time, some governments have recognised the possibility of gaining strategic advantages by tolerating their activities and have chosen either to ignore them or to allow them to operate discreetly, thereby limiting the risk of direct legal or diplomatic repercussions. In this context, these groups have become indirect instruments for advancing state interests. Consequently, a so-called *grey zone* has emerged, in which cybercrime intersects with geopolitical interests and cybercriminals act as indirect instruments of influence.

The use of cybercriminal networks as intermediaries can provide states with significant geopolitical advantages, as these networks can operate without direct attribution of responsibility to the states concerned. Thus, states can engage in economic sabotage, the theft of sensitive data, or attacks against critical infrastructure without publicly assuming

responsibility for such actions. The cyber dimension has become an arena in which hostile activities unfold alongside overt conflicts, contributing to their influence and escalation.

The relationship between state actors and cybercriminal groups highlights a transformation in the ways influence is exercised in cyberspace. States no longer act exclusively through direct means but may also resort to informal networks that are difficult to trace and attribute, which can become part of their indirect instruments of power projection. In this context, the capacity to employ or counter these networks may constitute an important strategic asset.

In a society characterised by accelerated digitalisation, conventional activities have become increasingly interconnected with cyberspace. Advances in information and communication technologies have brought considerable benefits but have simultaneously exposed every sector of state functioning to new vulnerabilities. Today, protecting data against malicious threats is no longer merely a technical concern but a fundamental necessity. Malicious code continues to evolve, as do cyberattacks, which can often infiltrate systems without the operators' knowledge and gain unauthorised access to their resources. Such intrusions are facilitated by increasingly sophisticated social engineering techniques that exploit Internet users' insufficient knowledge and awareness of the nature and scale of these threats.

Among these threats, ransomware attacks have evolved considerably, becoming one of the most persistent forms of cyberattack affecting global security today. From the perspective of cyberattackers, the Internet has served as the primary instrument for establishing an ecosystem in which financial networks can be developed and used to conduct activities through private or concealed channels, including the *dark web*. Within underground forums, attackers have been able to anonymise transactions and circumvent traditional monitoring and control mechanisms. The popularity of digital currencies, such as *Bitcoin*, has provided attackers with a considerable advantage by offering a pseudonymous payment method that has enabled them to monetise their extortion activities.

In recent years, cybercriminal groups have incorporated sophisticated business models known as *Ransomware-as-a-Service* (RaaS) syndicates, with the aim of maximising their profits. Under these models, individuals with basic technical skills can, in exchange for a fee, rent the infrastructure provided by a group and actively participate in conducting attacks. A percentage of the ransom payment subsequently goes to the administrators of the service. This proliferation of capabilities has significantly transformed the structure of the cybercrime ecosystem, directly influencing how these syndicates are currently perceived and analysed.

The information revolution has contributed to the emergence of new types of actors involved in conflicts, as well as to the diversification of the strategies they employ, directly influencing the ways in which states are affected by cyberattacks. Today, technology is

indispensable to the functioning of society and can influence almost every sector. For attackers, technology can represent a vulnerability to be exploited, meaning that critical infrastructure may become a target of sabotage operations, particularly in the context of armed conflicts. The relationship between warfare and cybercrime can be analysed by examining how these groups are involved, directly or indirectly, in the conduct of conflicts.

Cybercrime, whether perpetrated by state or non-state actors, has evolved into a threat to national security, as it targets critical sectors such as healthcare, education, financial systems, and the energy sector, among others. The gains derived from disrupting essential services may constitute a significant incentive for the continuation of cyberattacks. To understand the complexity of these groups, it is necessary to examine how they are organised. They operate through well-defined organisational structures in which each member performs a specific role.

Like any other cyber threat, the ransomware ecosystem is constantly evolving and adapting to new technologies, including through the use of artificial intelligence (AI) to enhance the efficiency of criminal activities. Today, large language models (LLMs) can be used to identify potential victims, draft ransom notes, and adapt them to the victim's language and cultural context, with the aim of increasing the likelihood of payment. Nevertheless, regardless of their profitability, competitiveness, and level of technical organisation, cybercriminal groups may be influenced by the geopolitical environment.

The invasion of Ukraine (*Україна*) marked a turning point in the reconfiguration of this ecosystem, as new political allegiances emerged. Thus, cybercriminal groups that had primarily pursued financial gains before the conflict became divided into camps supporting the belligerents, giving rise to pro-Russian and pro-Ukrainian factions. One example is the ransomware group *Conti*, which emerged in 2020 and publicly expressed its support for Russia's (*Россія*) invasion of Ukraine (*Україна*) on 25 February 2022, declaring its backing for Russia (*Россія*). It was the first ransomware group to publicly express support for a state actor, threatening to launch attacks against the critical infrastructure of any Western nation that intervened against Russia (*Россія*). This stance triggered a split within the group, prompting its Ukrainian affiliates to respond by disclosing substantial amounts of information, including internal communications and elements of its source code, thereby contributing to the group's subsequent disintegration.

The division of this criminal ecosystem along geopolitical lines highlights the fact that the actors involved no longer operate in an environment entirely separate from the dynamics of international geopolitics. These developments have contributed to a significant transformation of cybercrime, which, in certain circumstances, has come to reflect the geopolitical and ideological divisions generated by international conflicts. In this context, certain groups may come to be used as indirect instruments in forms of asymmetric warfare,

such as the war between Russia (*Россия*) and Ukraine (*Україна*).

This doctoral thesis investigates a phenomenon that has contributed to the transformation of the global security architecture: the involvement of cybercriminal groups in armed conflicts, whereby they move beyond exclusively financial objectives and adopt geopolitical positions, including through activities carried out in support of state actors. The research analyses the evolution of the ransomware ecosystem over the period 2020–2026 and examines how the invasion of Ukraine (*Україна*) by the Russian Federation (*Российская Федерация*), launched on 24 February 2022, contributed to a significant shift in the dynamics of asymmetric conflicts. In this context, the *Conti* group, previously oriented predominantly towards financial profit, expressed a geopolitical position and allegedly engaged in activities consistent with the interests of the Russian Federation (*Российская Федерация*), including forms of cooperation and strategic alignment. The overarching hypothesis of this research concerns the transformation of independent criminal groups into strategically aligned digital entities subordinate to the interests of the Russian Federation (*Российская Федерация*).

Historically, cybercriminal groups have operated predominantly in a discreet manner, avoiding the adoption of explicit geopolitical agendas in order to limit their exposure to law enforcement authorities and intelligence services. However, the Russo-Ukrainian conflict has revealed a shift in this operational approach, as certain actors involved in cybercrime have publicly adopted political positions and published political manifestos. This shift has created a need for a more in-depth examination of the phenomenon by analysing the factors that led the *Conti* group to publicly express its support for the Russian Federation (*Российская Федерация*) in the context of this conflict.

The aim of this thesis is to analyse a phenomenon that is emerging as a distinctive development in the history of cybercrime: the involvement of a ransomware group in, and its public expression of support for, the military conflict initiated by the Russian Federation (*Российская Федерация*) in Ukraine (*Україна*). The study seeks to analyse the dynamics of the ransomware ecosystem over a six-year period, as well as developments following the moment when the *Conti* group publicly declared its support for the Russian Federation (*Российская Федерация*). To support this investigation, three major groups within the ransomware cybercrime ecosystem are examined: *Conti*, *Black Basta*, and *The Gentlemen*. Their selection is based on the continuity identified among the actors involved in these groups, as evidenced in particular by information and discussions disclosed through data leaks. The analysis examines the movement of actors from one group to another, as well as the persistence of organisational and operational ties between these criminal ecosystems.

The *Conti* group is analysed as a relevant case study, as it was the first ransomware group to publicly express support for the invasion of Ukraine (*Україна*) by the Russian Federation (*Российская Федерация*). This position was followed shortly thereafter by the

disclosure of the group's internal communications, which revealed divisions among its members and the subsequent affiliation of some of them with other cybercriminal groups. Complementarily, the research examines a second group, *Black Basta*, identified as the operational successor to the *Conti* syndicate, and a third group, *The Gentlemen*, which exhibits operational continuity with the other groups.

The rationale for selecting these three cases stems from the similarities in their respective trajectories. Approximately three years after the Russian Federation's (*Российская Федерация*) invasion of Ukraine (*Україна*), *Black Basta* was itself affected by the disclosure of internal information, thereby facilitating a comparative analysis of actor continuity, organisational structures, and information security vulnerabilities within the groups under investigation. The third group, *The Gentlemen*, was also affected by the disclosure of internal information, providing a relevant documentary basis for analysing the relationships between cybercriminal groups and the interests of the Russian state.

The corroboration of information derived from these data leaks provides relevant evidence for testing the overarching hypothesis concerning the existence of forms of cooperation or alignment between the groups under investigation and Russian state actors. In this regard, the leaked messages contain information concerning links between members of cybercriminal groups and structures or intelligence services of the Russian Federation (*Российская Федерация*), such as the Federal Security Service of the Russian Federation (FSB) (*Федеральная служба безопасности Российской Федерации – ФСБ*).

To achieve its stated aim, the research pursues two major objectives designed to identify and explain these transformations.

Theoretical objective: To analyse the novelty of the implications of hybrid activities within cybercrime associated with the Russian Federation (*Российская Федерация*). Drawing on offensive neorealism, the thesis seeks to argue that the mobilisation of groups within the ransomware ecosystem in the context of the 2022 invasion constitutes a significant phenomenon for analysing how cyber actors can become committed participants in interstate conflicts. In this context, the research examines the implications of this transformation for the concept of *unpeace*.

Empirical objective: To map and graphically represent the organisational structures and the evolution of the actors involved in the *Conti*, *Black Basta*, and *The Gentlemen* groups. The research seeks to identify, represent, and analyse the hierarchies and roles of cyber actors on the basis of primary sources and internal communications disclosed on forums and other platforms used by cybercriminal communities. The analysis involves examining and translating messages written in Russian, as well as interpreting the context in which they were transmitted and their content, with the aim of identifying potential links between the ransomware groups under investigation and Russian state actors or structures. Furthermore,

the research seeks to identify continuity among actors, organisational structures, and operational relationships across the three groups, and to explain the mechanisms through which these transitions occurred.

The scientific rationale for selecting this research topic, concerning the cybercrime ecosystem, originates in a moment of systemic rupture observed in real time: the event initiated on 24 February 2022, namely the invasion of Ukraine (*Україна*) by the Russian Federation (*Российская Федерация*). Shortly after the invasion began, the leadership of the *Conti* ransomware group, which was considered at the time to be one of the most active and influential ransomware cybercriminal groups worldwide, published a statement expressing support for the Russian government. This position marked the beginning of the group's internal fragmentation, which culminated in the disclosure of internal communications by one of its members, a Ukrainian national who publicly opposed the group's position. The disclosure of these internal messages became known as the *Conti Leaks* and provided access to a substantial body of information concerning the group's organisational structure, relationships among its members, and operational methods.

At the international level, the academic literature on ransomware is extensive and is largely dominated by technical analyses focusing on the examination of malicious code characteristics, the techniques and procedures employed by cyber actors, and the mechanisms for preventing and mitigating the effects of these attacks. The topic addressed in this thesis extends this perspective by analysing the relationships between members of ransomware groups and Russian state actors, with particular emphasis on potential connections with the intelligence services of the Russian Federation (*Российская Федерация*).

Within the academic context, research on the cybercrime ecosystem associated with Russia's sphere of influence in the context of the war remains comparatively underdeveloped. Accordingly, this study seeks to demonstrate its original contribution through the following elements: the analysis of an event relevant to the study of cybersecurity and the examination of Russian-language communications contained in the *Conti Leaks*, *Black Basta Leaks*, and *The Gentlemen Leaks* archives, with a view to identifying relationships between the cyber actors under investigation and Russian state structures.

To structure the analytical approach and highlight the novel nature of the phenomenon, this thesis is designed as a qualitative, empirical, and exploratory study, based on a multiple and comparative case study design. The empirical nature of the research is supported by the use of primary sources, consisting of conversations between group members extracted from the *Conti Leaks*, *Black Basta Leaks*, and *The Gentlemen Leaks* archives, as well as discussions published on Dark Web forums. The translation of messages written in Russian required, where necessary, the interpretation of the specific slang used by cybercriminals, thereby facilitating the analysis of their intentions, practices, and strategies.

An original contribution of this research lies in the development of visual organisational charts representing the actors mentioned in the leaked materials. These representations make it possible to identify and visualise the internal structures, hierarchies, and roles assigned to actors within the groups under investigation, as well as to trace their movement and evolution across the *Conti*, *Black Basta*, and *The Gentlemen* groups.

The thesis establishes an explanatory link between neorealism, the analysis of the legal and institutional framework of the Russian Federation (*Российская Федерация*) through the concept of informal protection known as *krysha* (*крыша*), and qualitative research methods applied to digital environments. Given the clandestine nature of the actors under investigation, the methodological approach required the use of tools adapted to digital environments that are less accessible to the general public. The primary research method employed is netnography (online ethnography), applied to online communities associated with cybercrime, including Dark Web forums and Russian-language Telegram channels. The application of this method involved the systematic monitoring of these communities' activities, the examination of interactions between members, posts and published messages, and the observation of behavioural and organisational changes over time. This approach made it possible to identify interaction patterns, changes in members' positions, and the ways in which geopolitical events influenced the internal dynamics of these communities, particularly in the context of the invasion.

Netnography represents an essential research method for understanding how a community initially oriented exclusively towards profit became polarised along geopolitical lines. Netnography is structurally complemented by retrospective content analysis, applied to the data corpus derived from the *Conti Leaks* archive and the datasets associated with *Black Basta Leaks* and *The Gentlemen Leaks*. Through the translation and interpretation of the specific slang used by group members, the research seeks to identify relationships between these individuals and the Russian state, as well as to analyse their motivational profiles. The use of this corpus of leaked internal communications enables an examination of the groups' organisational structures, including leadership roles and the distribution of responsibilities. The research findings will contribute to understanding how cybercriminal activities can affect public institutions as well as individual citizens.

The research design adopted in this thesis stems from the need to move beyond a mere description of ransomware incidents and instead provide an in-depth analysis of the asymmetric power mechanisms that structure the relationships between cybercrime and the state apparatus of the Russian Federation (*Российская Федерация*). In the current context of international relations, characterised by increasingly blurred boundaries between the actions of state and non-state actors, the research examines how the Russo-Ukrainian war has influenced the positioning and involvement of certain ransomware groups in supporting the

invasion.

All information analysed is subjected to a rigorous process of verification and empirical corroboration by cross-referencing it with primary sources and information available in the leaked internal communications of the groups under investigation, subsequently corroborated by cybersecurity reports and institutions with relevant responsibilities in this field. More specifically, the research design focuses on identifying and analysing potential relationships between members of ransomware groups and individuals associated with the Russian state's intelligence services, as well as examining the mechanisms through which these relationships may be reflected in the activities and positioning of the groups under investigation. In this regard, the research focuses on the concepts of functional symbiosis and strategic instrumentalisation, examining how relationships between cyber actors and state actors may extend beyond the exclusively financial dimension. The central issue does not lie in monetary transactions themselves, but in the possibility of outsourcing forms of asymmetric aggression to non-state actors.

In this context, the research question guiding this thesis is: *How did the Russian Federation's invasion of Ukraine transform the ransomware criminal ecosystem?* The research proceeds from the premise that, following the launch of the invasion, part of the ransomware ecosystem ceased to operate exclusively on a financial basis and also adopted geopolitical positions, including through the public expression of support for one of the parties involved in the conflict, in this case, the aggressor. This transformation can be analysed through the relationship between cybercrime, geopolitical dynamics, and forms of hybrid warfare, as well as through its implications for the assessment of emerging cyber threats.

For the empirical investigation, leaked archives of internal communications constitute particularly relevant primary sources, as they allow for the direct and detailed examination of interactions between group members, organisational structures, and operational practices. The recurrence of a similar phenomenon involving the exposure of internal messages approximately three years apart, in February 2025 and subsequently in May 2026, provides an opportunity for comparative analysis and strengthens the empirical relevance of the research. Across the three data leaks, information can be identified concerning the identities of certain individuals associated with the groups, the ways in which they retained their aliases and attack methods, and their movement from one group to another.

The relevance of this research lies in the need to analyse the mechanisms through which the concept of plausible deniability may operate in the relationship between state actors and cybercriminal groups. In this context, the research examines the extent to which relationships, forms of cooperation, or instances of tolerance between the groups under investigation and Russian state actors or structures may contribute to the emergence of a

model of cybercrime associated with state interests, with implications for the contemporary architecture of global cybersecurity.

Hypothesis 1: *The outbreak of the conflict on 24 February 2022 acted as a catalyst for the fragmentation of the Russian-speaking ransomware ecosystem, prompting a transition from an exclusively financially motivated operating model to one oriented towards supporting the geopolitical interests of the Russian Federation.*

Hypothesis 2: *Informal cooperation between members of cybercriminal groups and members of Russian intelligence services operates as a mechanism of conditional reciprocity, whereby support for the invasion of Ukraine becomes a prerequisite for maintaining operational impunity from law enforcement.*

The selection of cases examined in this research follows a theoretical rationale grounded in the case selection criteria proposed in the methodological literature, including the works of *Gerring* and *Yin*. The focus on ransomware, rather than on other forms of cyber threats, such as cyber espionage, is justified by its position at the intersection of the underground economy and national security. Among the distinctive characteristics of the ransomware ecosystem is the existence of visible forms of communication and public interaction through leak sites, negotiation channels, and forums used by cyber actors. These characteristics have enabled the identification of relevant primary sources for investigating transformations within the ecosystem, including the ways in which predominantly financial motivations may intersect with geopolitical and ideological positions.

To ensure a high level of internal validity in the multiple-case study, the *Conti* and *Black Basta* groups have been selected to examine two distinct stages in the evolution of the Russian cybercrime ecosystem. In addition, the case of *The Gentlemen* demonstrates that, although cybercriminal groups may be dissolved, the activities and operational continuity of their members can be maintained through their migration to other criminal structures. The *Conti* case serves as a reference point for understanding how a complex cybercriminal organisational structure was affected by the adoption of an explicit political position. The analysis of *Conti* is essential because it provides a dataset of exfiltrated information (*Conti Leaks*), originating from the group's internal communications and disclosed in the context of the Russo-Ukrainian invasion in February 2022. Through the analysis of this case, the research seeks to examine the relationship between the group's political stance, its internal structure, and potential forms of influence or control exercised over it by state actors.

The *Black Basta* case has been selected to examine the continuity of actors and operational practices previously associated with the *Conti* group, given the numerous similarities between them. This case makes it possible to observe the reorganisation of the cybercrime ecosystem and to examine how certain organisational and operational elements have been maintained or transformed. Approximately three years after *Conti* publicly

expressed its support for the Russian side, the second group, *Black Basta*, was itself affected by the disclosure of its internal communications. The published data provide an opportunity for a complex comparative analysis of the evolution of the reorganised structure, operational continuity, and exposure risks. The comparative approach enables the research to move beyond the limitations of a single-case analysis and examine systemic evolution towards more decentralised and adaptable forms. Case selection is therefore intended not only to explain individual events but also to analyse the systemic transformation of the threat in the context of geopolitical pressures associated with the Russian state.

A fundamental requirement for ensuring methodological rigour is the establishment of fixed temporal reference points that allow the evolution of the phenomenon to be analysed independently of the volatility of external events. Accordingly, the research is delimited to the period 2020–2026, an interval that allows for the examination of the evolution of actors and activities within cybercriminal communities. The observation covered Dark Web cybercrime forums, public websites associated with the groups under investigation, as well as Telegram and TOX channels used for internal communication. Within this period, 2021 represents an important contextual reference point, marked by the publication by Vladimir Putin (Владимир Владимирович Путин) of the essay “Об историческом единстве русских и украинцев” (“On the Historical Unity of Russians and Ukrainians”), which advanced a series of historical and political arguments concerning the relationship between Russia (Россия) and Ukraine (Україна). In this research, the document is analysed as an element of the discursive framework that preceded the invasion, rather than as a direct cause of the mobilisation of cybercriminal actors. As an operational reference point, *T0* is established as 25 February 2022, the date on which the *Conti* group publicly expressed its support for the Russian government, one day after the invasion began.

The temporal delimitation makes it possible to structure the analysis into several stages. The first stage covers the period 2020–2022 and examines the evolution of the *Conti* group up to the point at which it adopted its public position and the subsequent disclosure of its internal communications. The second stage examines the period of reorganisation and continuity among actors within the ransomware ecosystem, focusing on the *Black Basta* group. A second empirical reference point is 11 February 2025, the date on which *Black Basta*’s internal communications were disclosed, covering primarily the period from September 2023 to September 2024. The third stage consists of the post-disclosure assessment and the examination of *The Gentlemen Leaks*, dated 13 May 2026. The final stage of the research examines developments following these events up to the end of the observation period, in September 2026. This temporal delimitation allows the observation period to be used as a control parameter for cross-case comparison, facilitating the analysis of actor continuity, organisational changes, and transformations in the activities of the groups under

investigation. Thus, the research does not limit itself to analysing isolated events but instead examines the evolution of the cybercrime ecosystem over a defined period, in relation to the principal instances of dissolution and reorganisation identified empirically.

The research methodology is qualitative, empirical, and exploratory, grounded in a multiple and comparative case study design. The empirical validity of the research is supported by a data triangulation strategy employed to verify and corroborate information derived from different sources and data types. This methodological framework makes it possible to distinguish between static data, information obtained from data leaks, and data relating to the current dynamics of the ecosystem, with each category being analysed using methodological tools appropriate to its specific characteristics.

A major component of the empirical material consists of extensive datasets exfiltrated from the infrastructures of the groups under investigation, known as *Conti Leaks*, *Black Basta Leaks*, and *The Gentlemen Leaks*. These archives constitute primary research sources and provide direct access to the groups' internal communications. The analysis of conversation logs, available in formats such as *Jabber* and *JSON*, as well as of internal documents and protocols concerning the organisation and conduct of activities, is carried out through retrospective qualitative content analysis. This method enables the identification and interpretation of recurring themes, relationships between actors, organisational roles, and changes occurring within the groups under investigation. This approach makes it possible to analyse, on the one hand, the structure of the *Conti* group, which was no longer active when the research commenced, and, on the other hand, the structures of *Black Basta* and *The Gentlemen*, whose activities could be monitored while they were operational. In the latter cases, corroborating information from public sources with subsequently disclosed data provided empirical evidence for testing the hypothesis concerning the continuity of certain actors originating in the *Conti* ecosystem within the new organisational structure.

Between 2022 and 2026, the analysis of messages published on forums associated with cybercriminal communities and of cybersecurity reports issued by specialised companies enabled the identification of relationships and continuities among the actors under investigation. Subsequently, information derived from data leaks made it possible to verify and corroborate these connections. The disclosed data provided access to information concerning internal recruitment mechanisms, hierarchical relationships and the distribution of roles, as well as interactions between group members and certain individuals or entities for which there are indications of connections with Russian intelligence structures or services.

Treating these communications as digital archives enables the research to maintain a fixed and verifiable empirical corpus to which systematic analytical and corroboration procedures can be applied. In this way, data derived from leaked communications can be compared with information obtained through netnographic observation and secondary

cybersecurity sources, thereby helping to reduce the risk of interpretations based exclusively on isolated observations. Unlike the analysis of leaked internal communications, netnography is employed in this thesis as a tool for monitoring the dynamics of the cybercrime ecosystem on underground forums, such as *XSS*, *Exploit*, and *RAMP*, over the period 2022–2026. The method is applied to analyse how community members interact, discuss, and collaborate, as well as to examine messages published in areas accessible to members of these forums.

In the capacity of a non-participant observer, the research examined public and semi-public discussions between Initial Access Brokers (IABs) and ransomware operators, as well as interactions among individuals involved in recruiting new members or publishing advertisements and messages on forums. The systematic monitoring of these interactions enabled the compilation of an observational corpus based on the communication styles, interaction patterns, behaviour, and activities of the actors under investigation.

An important objective of applying netnography is to observe the self-regulatory mechanisms operating within these communities. In this regard, the research examines, for example, how certain moderators imposed restrictions following the outbreak of the invasion on the publication of messages concerning entities within the CIS (Commonwealth of Independent States), information about the arrests of community members, or opinions regarding the conduct of the war. These rules and moderator interventions provide indications of the internal mechanisms of control, self-regulation, and maintenance of community norms.

The distinction between analysing leaked communications as historical documents and monitoring forums as a netnographic environment enables the research to capture both the evolution of the groups under investigation and the behaviour and interactions of actors during the period in which these groups were active. Corroborating these two perspectives provides a broader empirical basis for analysing organisational and geopolitical transformations within the cybercrime ecosystem, moving beyond a purely technical analysis of attacks. The selection of the forums under investigation is justified by their relevance to the cybercriminal communities being studied and by the volume and diversity of information available for the period under examination.

To ensure the scientific rigour of the research and avoid ambiguities identified in previous evaluations, this study proposes an operationalisation framework for the central concepts. Within the present study, the concept of “strategic instrumentalisation” is operationalised through empirical indicators observable in the collected data, which enable the identification and analysis of the specific ways in which cybercriminal actors may be integrated into the pursuit of geopolitical objectives. In this regard, the concept of a “shift from profit to patriotism” is broken down into two fundamental dimensions: the motivational dimension, which concerns changes in the objectives and motivations of the actors, and the operational dimension, which concerns changes in their behaviour and activities in the context

of the Russo-Ukrainian conflict.

With regard to data processing and interpretation, the research employs *Process Tracing* to analyse not only the existence of a temporal association between the war and the behavioural transformations of cybercriminal groups, but also the mechanisms through which this transformation occurred. The research seeks to reconstruct the sequence of events and identify the causal mechanisms that may explain the relationship between the independent variable, represented by the normative and operational pressures associated with the Russian state, and the dependent variable, represented by changes in the behaviour and positioning of cybercriminal groups.

The application of this method involves the use of rigorous evidentiary tests, such as the “smoking gun test” and the “hoop test”. For example, the analysis of the *Conti Leaks* chats will seek evidence of specific interactions that function as a mechanism for enforcing state directives, such as tasks received through intermediaries or references to immunity from prosecution granted in exchange for carrying out specific attacks or participating in volunteer initiatives. This method will make it possible to determine whether the behavioural changes observed in these groups resulted from organic evolution or, as hypothesised in this thesis, from the association of certain members with the Russian government.

The use of *Process Tracing* makes it possible to move beyond a strictly descriptive narrative and direct the analysis towards identifying the mechanisms through which geopolitical transformations and pressures associated with the Russian security environment may have influenced the decisions and behaviour of cybercriminal actors. This approach addresses the need to ground the research conclusions in a systematic analysis of the sequence of events, relationships between actors, and causal mechanisms identified within the empirical corpus. In summary, the proposed methodological framework seeks to strengthen the internal validity of the research. Corroborating primary sources, netnographic observations, and secondary sources provides an analytical framework for examining the reconfiguration of the cybercrime ecosystem in the context of geopolitical transformations and the Russo-Ukrainian conflict.

The thesis is structured into four main chapters, arranged in a logical and progressive sequence that develops the theoretical and conceptual framework, establishes the methodological foundations of the research, and applies them to the contemporary ransomware cybercrime ecosystem. The structure enables a progression from the analysis of theories and concepts relevant to understanding cyberspace and transformations in international relations, through the definition and justification of the methodological design, to the empirical examination of the dynamics, organisational structures, and behavioural transformations of the ransomware groups under investigation. In this way, the four chapters complement one another in establishing the analytical framework required to examine the

relationships between cybercrime, geopolitical transformations, and the state actors involved in the Russo-Ukrainian conflict.

Chapter I, entitled “*Theoretical and Conceptual Foundations: The Geopolitics of Cyberspace*”, establishes the literature review and theoretical foundations of the research, examining how classical theories of International Relations, such as Structural Realism and Offensive Neorealism, adapt to the anarchy characteristic of the digital environment. Within this framework, cyberspace is conceptualised as a domain of geopolitical conflict in which the security dilemma is exacerbated by the structural advantage enjoyed by the offensive and by the diminishing constraints imposed by geography. The chapter also examines a reconceptualisation of cybercrime, reframing it from a private financial offence into an act of hybrid warfare conducted within the “grey zone” of international relations. Finally, it analyses the *Doctrine of the Russian Federation* (Доктрина Российской Федерации) concerning cyber sovereignty, *RuNet* (PyHem), and the informal protection system known as *krysha* (крыша), demonstrating how the Kremlin (Кремль) militarises the information environment through the strategic instrumentalisation and co-optation of proxy actors.

Chapter II, entitled “*The Russian Cybercrime Ecosystem: The Convergence of Profit and Strategic Objectives*”, marks the transition from the theoretical framework to the operational realities of the Russian digital environment, investigating the technical, financial, and legal infrastructure underpinning asymmetric aggression. The chapter analyses the Russian Federation’s (Российская Федерация) digital sovereignty paradigm, *RuNet* (PyHem), and the mechanism of “selective law enforcement”, demonstrating how the impunity afforded under Article 61 of the Russian Constitution (Статья 61 Конституции Российской Федерации) and the informal protection guarantee (*krysha* – крыша) are conditioned on attacks being directed exclusively outside the Commonwealth of Independent States (CIS) (Содружество Независимых Государств). The chapter examines the channels of the underground economy, ranging from the cryptocurrency laundering ecosystem and Dark Web marketplaces (*RAMP*, *XSS*, and *Exploit*) to the essential role of Initial Access Brokers (IABs) in the *Access-as-a-Service* model. It also examines the systemic reconfiguration triggered by the invasion of 24 February 2022, marking the transition from financial opportunism to patriotic mobilisation and alignment with *New Generation Warfare* (NGW) (Война следующего поколения).

Chapter III, entitled “*A Comparative Analysis of the Ransomware Ecosystem: The Cases of Conti and Black Basta*”, constitutes the empirical core of the thesis and explores the evolution and systemic reorganisation of the threat through a multiple and comparative case study. Grounded in the application of *Process Tracing*, netnography, and the theoretical framework of dissipative structures (Илья Пригожине – Илья Пригожин), the chapter reconstructs the causal sequences linking geopolitical pressure exerted by the Kremlin

(*Кремль*) to the subservient conduct of cybercriminals. The analysis traces the transition from the organisational and ideologically oriented model of the *Conti* syndicate—whose public alignment triggered internal fragmentation and the *Conti Leaks*—to the decentralised, adaptive, and resilient model of the *Black Basta* group (*Black Basta Leaks*). Through the translation and decoding of Russian-language primary sources, including the criminal slang known as *fenya* (*феня*), the chapter reveals hierarchical relationships, extortion mechanisms, cryptocurrency laundering networks (*Garantex*, *Media Land*), and links between group leaders and Russian intelligence services (FSB and GRU). The empirical originality of the research is further demonstrated through the construction of operational organisational charts of the syndicates and the identification of the real names of key operators, such as *Oleg Nefedov* (*Олег Неведов*)—*GG/Tramp*—and *Vitaly Kovalev* (*Виталий Ковалёв*)—*Stern/Bentley*.

Chapter IV, entitled “*The Ransomware Ecosystem and Its Evolution*”, concludes the analytical investigation by providing an assessment of the prospective dynamics of cyber threats over the 2025–2026 period and evaluating the impact of emerging technologies on national security. The chapter investigates the consolidation of the *Ransomware-as-a-Service* (RaaS) model and double extortion, analysing the third empirical case study, conducted in May 2026, concerning the *The Gentlemen* group (*The Gentlemen Leaks*). The analysis of internal chats reveals a transition towards experienced networks composed of small cores of veteran operators and affiliates attracted by particularly aggressive profit-sharing models. The chapter also explores the disruptive role of generative artificial intelligence, including *WormGPT*, *FraudGPT*, and *PromptLock*, described as an early AI-based ransomware strain, in automating social engineering, overcoming language barriers, generating malicious code in real time, and rapidly analysing exfiltrated data. The second part conceptualises the pillars of Cyber Intelligence (*CYBINT*, *OSINT*, and *SOCMINT*) as essential tools for anticipating and strategically analysing asymmetric attacks. Finally, the chapter evaluates international cooperation mechanisms, the role of *Active Disruption* operations, such as *Operation Endgame* conducted by Europol, and the framework of cyber diplomacy in counteracting the impunity afforded by states that shelter members of cybercrime syndicates and provide them with operational support or strategic advantages.

CONCLUSIONS OF THE THESIS

This doctoral thesis investigated a defining phenomenon that has reshaped the contemporary global security architecture: the point at which cybercriminal groups abandoned financial neutrality and became actively and explicitly involved in a kinetic war, acting as proxies for a state actor. The research demonstrated that cyberspace no longer represents merely a neutral communications infrastructure but has become one of the most volatile and active arenas of geopolitical competition, reshaping the balance of power between state and non-state actors. Ransomware has moved beyond the boundaries of traditional financial crime, evolving into a national security concern and an essential instrument of hybrid and asymmetric warfare.

The empirical investigation, grounded in netnographic analysis and the application of *Process Tracing* to primary sources, including the *Conti Leaks* and *Black Basta Leaks* archives, addressed the research question and provided evidence that the Russian state exploited the anarchy of cyberspace to obtain strategic advantages. The findings highlighted the process through which the Kremlin created a “grey zone” in which criminal interests intersected with the objectives of Russian military doctrine. This zone enabled Russia to externalise asymmetric aggression to cyber proxies while maintaining plausible deniability on the international stage.

This transformation was driven by the integration of the criminal ecosystem into Russia’s information confrontation strategy. By employing these groups as indirect instruments of power, Russia targeted critical Western sectors, including healthcare, energy, and logistics, to inflict economic sabotage and psychological subversion, thereby substantially blurring the boundary between peace and open conflict. The answer to the research question highlights that, following the outbreak of the war, attackers no longer pursued extortion exclusively but also contributed to a state of *unpeace* intended to disrupt the functioning of institutions in countries supporting Ukraine.

The thesis formulated and tested two major hypotheses, both of which were confirmed by the empirical analysis of internal communications and the structural dynamics of the groups under investigation.

Validation of Hypothesis 1: The outbreak of the conflict on 24 February 2022 acted as a catalyst for the fragmentation of the Russian-speaking ransomware ecosystem, prompting a transition from an operating model exclusively oriented towards financial gain to one focused on supporting the geopolitical interests of the Russian Federation. This hypothesis was fully validated through the case study of the *Conti* group. The war in Ukraine acted as a systemic turning point, dispelling the myth that cybercrime operates independently of political considerations. On 25 February 2022, just one day after the invasion, the leadership of *Conti*

published a statement on its own blog declaring its full support for the Russian government and threatening destructive attacks against the critical infrastructure of adversaries that retaliated. This explicit shift from profit to patriotism invalidated the principle of neutrality and immediately triggered a major internal fracture. The division of the ecosystem along ideological and nationalist lines was demonstrated by the *Conti Leaks* incident: a Ukrainian cybersecurity researcher retaliated against the pro-Russian leadership by publishing more than 170,000 internal chat logs, exposing the architecture of the entire group. The hypothesis is therefore confirmed: the cyber ecosystem is no longer united solely by economic motives but has undergone an organic fragmentation into opposing camps supporting the belligerents, confirming its transformation into an asymmetric and ideologically driven instrument of warfare.

Validation of Hypothesis 2: Informal cooperation between members of cybercriminal groups and members of Russian intelligence services operates as a mechanism of conditional reciprocity, whereby support for the invasion of Ukraine becomes a prerequisite for maintaining operational impunity from law enforcement. The hypothesis was empirically validated through the identification of the operation of a mafia-style protection mechanism known as *krysha* (“roof”). The Russian state guarantees cybercriminals protection against extradition by invoking Article 61 of the Constitution of the Russian Federation and selectively enforces Articles 272 and 273 of the Criminal Code. This informal social contract provides comprehensive protection from the Federal Security Service (FSB), provided that hackers adhere to the strict rule of not attacking targets within the Commonwealth of Independent States (CIS). Moreover, even when domestic arrests occur, as in the case of the *REvil* group, they often serve as a mechanism for co-opting and forcibly recruiting specialists into intelligence structures, effectively enabling the state to appropriate cybercriminal capabilities.

The leaked archives provided evidence of subordination and cooperation between group leaders and the FSB/GRU. The *Conti Leaks* revealed that the leader known as *Stern* worked for the FSB, that members operated in the vicinity of FSB headquarters in Moscow and St Petersburg, and that they discussed requests originating from intelligence agencies, including cooperation with government-backed advanced persistent threat (APT) groups referred to as the “Bears” (*APT29/Cozy Bear*) and the surveillance of journalists investigating the government, including in connection with the Navalny case. Similarly, the release of *Black Basta* data in 2025 confirmed the continuity of this pattern of systemic corruption: the group’s leader, Oleg Nefedov (*GG/Tramp*), explicitly acknowledged in TOX messages that he had bribed officers from the Lubyanka (FSB) and the GRU to secure protection. Following his detention in Armenia, a “green corridor”, allegedly facilitated by influential individuals within the Russian leadership, enabled his immediate transfer to Moscow, according to

information derived from the analysed conversations. This evidence indicates that state-backed impunity may be embedded at the highest levels of the political system.

A fundamental component of the research involved analysing the structural evolution of the Russian-speaking cybercrime ecosystem. To explain how this ecosystem survived large-scale data exposures (*leaks*) and international sanctions, the thesis applied the concept of dissipative structures. From this perspective, cybercriminal syndicates function as complex systems operating far from equilibrium. At times of critical crisis or fragmentation, such as the *Conti Leaks* incident triggered by the invasion of Ukraine, these systems do not necessarily disintegrate permanently but instead reorganise into new, more flexible and adaptive forms. Triangulation of data from primary sources (*Conti Leaks* and *Black Basta Leaks*) made it possible to trace this transition from monopolistic, semi-corporatised structures to decentralised and highly persistent networks.

The research demonstrated that the *Conti* group represented the culmination of organisational maturity within the ransomware ecosystem. Having moved beyond the traditional model of small hacker groups, *Conti* operated according to a fully integrated corporate business model capable of generating estimated annual profits amounting to hundreds of millions of US dollars. The analysis of internal conversations revealed a rigid organisational chart and a clear division of labour: human resources (HR) departments that actively recruited personnel through forums, such as Moscow-based *headhunting.ru*; programming teams (coders); penetration testing specialists; OSINT experts responsible for victim profiling; and a team of negotiators (callers). Employees received fixed salaries, paid in Bitcoin, performance evaluations, annual leave, and performance-based bonuses. Leaders such as *Stern*, *Target*, *Tramp*, and *Mango* managed substantial budgets, coordinated dozens of affiliates, and even intended to establish their own social networks on the Dark Web, such as the *matrioska.ru* project, and cryptocurrency exchange platforms, such as *Bablo*, to facilitate money laundering.

Furthermore, the research challenged the myth of the isolated hacker: senior *Conti* members operated from physical offices located in Moscow and St Petersburg and frequently travelled to Dubai for meetings. Despite achieving unprecedented financial success, the group's declared pro-Russian ideological alignment on 25 February 2022 triggered internal fragmentation, resulting in the publication of more than 168,000 internal messages and, ultimately, the official shutdown of the *Conti* brand in May 2022. This closure did not signify the disappearance of the threat, demonstrating the structural resilience of the ecosystem. The response to this crisis was immediate reorganisation under new identities. Emerging in April 2022, only a few weeks after the *Conti* data disclosures, the *Black Basta* group was empirically identified as its direct successor. The research validated this continuity by identifying the same key members operating under new aliases. For example, *Tramp*, a

principal operator within *Conti*, led *Black Basta* under the pseudonym *GG*, later identified as Oleg Nefedov, and was associated with more than 80,000 coordination messages.

Black Basta inherited the operational infrastructure, double-extortion tactics, money-laundering networks, including *Garantex*, and preference for targeting the same critical Western infrastructure, while maintaining the strict rule against attacking countries within the Commonwealth of Independent States (CIS). Nevertheless, *Black Basta* demonstrated a refinement of its social engineering techniques, employing voice phishing (vishing) and social engineering attacks through Microsoft Teams. Its operators impersonated help-desk teams to persuade employees to install remote-access applications such as AnyDesk. Although *Black Basta* attempted to compartmentalise its operations more effectively to avoid the fate of *Conti*, the criminal ecosystem remained vulnerable to internal tensions. This culminated in the *Black Basta Leaks* in February 2025, when approximately 197,000 messages were exposed, once again revealing the identities of group leaders and contributing to arrests, including that of Nefedov.

A recent case study dated 4 May 2026 reflects the current stage in the evolution of the ecosystem: the shift towards smaller, highly specialised, and exceptionally agile structures. Emerging in May 2025 following a financial dispute within the *Qilin* group, the *The Gentlemen* operation marks a new paradigm in the *Ransomware-as-a-Service* (RaaS) model. The research reveals that cybercriminals have learned from the vulnerabilities of the *Conti* organisational structure and adapted accordingly. *The Gentlemen* operates through a small core of approximately nine operators centred around the administrator *zeta88* (*hastalamuerte*). The group's agility is demonstrated by the speed of its operations: *zeta88* developed the RaaS administrative panel in just three days with the assistance of artificial intelligence. To attract the most experienced affiliates from rival syndicates, *The Gentlemen* aggressively modified its economic model, offering affiliates up to 97% of the revenue generated through data extortion without encryption and 90% of the proceeds from conventional ransomware attacks.

In terms of tactics, the group abandoned the continuous acquisition of zero-day vulnerabilities in favour of an opportunistic approach, efficiently exploiting the underground market for stolen credentials obtained through infostealers by scanning logs to gain access to vulnerable VPNs and corporate portals. The case of *The Gentlemen*, whose data were also disclosed in May 2026, demonstrates the extreme fluidity of the contemporary market: a dissatisfied affiliate today may establish and manage a leading RaaS syndicate tomorrow. The ecosystem is no longer controlled by a handful of cartels but by interconnected networks capable of dissolving and reorganising under a new brand while maintaining a sustained pace of attacks against global critical infrastructure, including targets in Romania.

Another major conclusion of the research concerns the logistical architecture of the criminal ecosystem. The thesis demonstrated that the effectiveness of ransomware groups

derives not exclusively from malicious code but also from a highly structured division of labour and a complex supply chain operating on the Dark Web. Contemporary asymmetric warfare is being industrialised through the *Access-as-a-Service* and *Ransomware-as-a-Service* (RaaS) models. The research highlighted that Initial Access Brokers (IABs) have become essential to cyber offensives. They act as specialised intermediaries: they compromise target networks through phishing, brute-force attacks, or the exploitation of vulnerabilities in virtual private network (VPN) infrastructure and the Remote Desktop Protocol (RDP), but do not encrypt the data themselves. Instead, they sell access to RaaS syndicates through exclusive Russian-language forums, including *RAMP*, *XSS*, and *Exploit*.

The observed dynamics indicate a transition towards business-to-business (B2B) relationships and vertical integration. For example, the *Conti Leaks* logs revealed how *Conti* leaders directly negotiated ransom-sharing arrangements with brokers such as *RDPCorp*. By outsourcing the intrusion stage, syndicates reduce execution times from months to just a few days, limiting the response time available to security institutions. From a financial perspective, the research concludes that these groups are heavily dependent on specialised platforms for laundering proceeds derived from extortion, employing the conventional three-stage process of placement, layering, and integration. The shift from Bitcoin to cryptocurrencies offering a higher degree of anonymity, such as Monero, together with the use of cryptocurrency mixing services (*tumblers*), demonstrates their adaptation to international monitoring efforts.

Both *Conti* and *Black Basta* used the Russian cryptocurrency exchange Garantex, subsequently sanctioned by the United States, to launder tens of millions of US dollars. One novel finding presented in this thesis is the emerging use of non-fungible tokens (NFTs) to launder funds, as well as the groups' dependence on "money mules" (drop accounts) recruited through Telegram, including through the *Laundromat* service, to convert illicit proceeds into fiat currency. The research also identified the intention of *Conti* leadership, through the aliases *Mango* and *Stern*, to establish its own social network and cryptocurrency platform on the Dark Web (*matrioska.ru/Bablo*), with the aim of controlling the entire money-laundering chain and reducing dependence on intermediaries vulnerable to sanctions.

Another conclusion concerns the profound technological adaptation undergone by the ecosystem during the 2025–2026 period, namely the transition from manual attacks to the automation of offensive operations through artificial intelligence (AI). The thesis substantiates the finding that AI now functions as an asymmetric force multiplier in information confrontation. Russian-speaking cybercriminals have moved beyond the use of legitimate commercial models, such as ChatGPT, and have developed their own AI systems without ethical restrictions. The research documents the emergence of underground large language model (LLM) tools, including *WormGPT*, *FraudGPT*, *DarkBERT*, and *ChaosGPT*. These

tools enable the automated generation of malicious code and the creation of grammatically and contextually accurate phishing and spear-phishing campaigns, removing language barriers for Russian-speaking hackers.

The direct adoption of AI by the groups under investigation was also observed. *Black Basta* developed its own internal chatbot, known as *BlackBastaGPT*, while *The Gentlemen* uses AI assistants, such as *DeepSeek* and *Qwen*, for code development and plans to employ AI to process and rapidly analyse vast volumes of exfiltrated data for targeted extortion. Furthermore, a turning point was identified in the 2025 release of *PromptLock*, described as the first AI-based ransomware strain, capable of generating malicious scripts in real time and dynamically adapting to the victim's defensive mechanisms.

In line with the Gerasimov Doctrine concerning information and psychological warfare, AI is used to erode trust in democratic societies. The use of deepfake technologies (audio and video) and voice cloning for vishing enables attackers to impersonate real individuals. As observed in the case of *Black Basta*, the group implemented vishing techniques through Microsoft Teams, calling employees and impersonating IT help-desk personnel to persuade them to download the malicious payload. The integration of AI automates the social engineering stage, substantially accelerates the intrusion process, and transforms the extortion model. AI chatbots are now also used to negotiate ransom payments directly with victims, maintaining a high level of psychological pressure without requiring direct emotional involvement or human effort on the part of the attacker. These innovations indicate that, for the Russian Federation, AI represents a cornerstone of the transition towards New Generation Warfare (NGW), providing an ideal instrument for disrupting decision-making processes in NATO member states while avoiding the kinetic threshold associated with Article 5.

Although the methodological framework of this doctoral thesis was rigorously grounded in data triangulation, employing netnography and *Process Tracing* directly on primary sources in the form of data leaks, the research acknowledges the existence of objective limitations. These limitations stem inherently from the clandestine, highly secured, and volatile nature of the Russian cybercrime ecosystem under investigation. First, one limitation concerns the impossibility of analysing interactions conducted in the physical, offline environment. Although digital data made it possible to reconstruct a detailed organisational chart and communication networks, a significant proportion of the activities and strategic negotiations undertaken by senior members took place face to face, in physical offices in Moscow and St Petersburg or during their travels to locations such as Dubai. These face-to-face meetings directly influence group dynamics and organisational decisions, aspects that cannot be fully captured through the analysis of digital footprints alone.

Second, structural difficulties persist in attributing cyberattacks and establishing

evidence of state-issued orders. The cyber environment is characterised by anonymity and provides state actors with the tactical advantage of plausible deniability. Although internal message archives provide evidence of clear associations and cooperation with FSB or GRU officers, including the subordination of leaders such as *Stern* and *Bentley*, the deliberate blurring of the boundary between opportunistic attacks and sabotage directly coordinated by the Kremlin remains a barrier to security analysis.

Third, the research's dependence on static leak databases, such as *Conti Leaks* and *Black Basta Leaks*, constitutes a temporal limitation. Although these documents represent a unique research opportunity, they provide only chronological snapshots of an extremely dynamic and complex ecosystem, covering, for example, 2020–2022 for *Conti* and 2023–2024 for *Black Basta*. Criminal groups frequently modify their tactics, techniques, and procedures (TTPs) and rapidly rebrand themselves to evade law enforcement monitoring.

Fourth, direct access to group members through messages in internal Telegram and TOX groups or on Russian-language forums was limited. These individuals are highly discreet and do not readily share information with outsiders. Nevertheless, there have been cases in which members of certain groups granted interviews to prominent researchers specialising in cybersecurity analysis. However, members of the groups examined in this thesis were not interviewed as part of the present research.

The rapid transformation of the cybercrime ecosystem and its growing interconnectedness with geopolitical instruments open up multiple research avenues necessary for the future development of cybersecurity studies. Analysing newly emerging successor groups and the internationalisation of ransomware represents an important direction for future research. Further studies should examine the dynamics of emerging and flexible groups such as *Akira*, *Royal*, *Qilin*, and *RansomHub*, investigating how affiliates migrate between these networks. The internationalisation of this model also warrants further investigation, as forecasts indicate that ransomware actors operating outside the Russian Federation may eventually outnumber their Russian counterparts, further fragmenting the global security architecture.

The evolution of malicious LLMs, such as *WormGPT* and *FraudGPT*, and the deployment of the first AI-based ransomware, *PromptLock*, represent only the beginning. Future research should assess the impact of autonomous AI agents on hybrid warfare, particularly in scenarios in which they could simultaneously coordinate disinformation operations involving deepfakes and sabotage against physical infrastructure, including logistics systems and energy networks, to trigger societal disruption. Furthermore, the evolution of post-quantum cryptography requires strategic investigation, as its adoption by cybercriminals could render data decryption impossible without payment of the ransom.

Another research direction concerns the assessment of the effectiveness of cyber

diplomacy instruments and *Active Disruption* measures. Future studies should examine the effectiveness of transnational law enforcement operations, such as Europol's *Operation Endgame*, in affecting the resilience of Dark Web networks. It is essential to investigate the impact of diplomatic instruments, such as the EU Cyber Diplomacy Toolbox, and the United Nations Convention against Cybercrime on translating technical attribution into tangible political costs and sanctions for states that guarantee immunity to hacker groups.

A final research direction concerns monitoring the most persistent ransomware groups from 2026 onwards. As demonstrated by *Conti* and *Black Basta*, these groups may themselves be compromised, potentially resulting in the online disclosure of internal information concerning other groups, as occurred in the case of *The Gentlemen* in May 2026. Consequently, studying these groups and analysing their operational methods constitutes an important avenue for future research.

In summary, this doctoral thesis demonstrates that cyberspace has moved beyond its status as neutral technological infrastructure to become a principal theatre of asymmetric operations and geopolitical competition in the twenty-first century. Historically examined through the lens of criminology as a straightforward financial crime involving extortion, ransomware has evolved into a national security concern and an instrument of hybrid warfare. The research substantiates the premise that the invasion of Ukraine by the Russian Federation, launched on 24 February 2022, acted as a systemic turning point. This event dispelled the myth of the apolitical independence of Russian-speaking cybercrime, triggering an ideological fracture that compelled Ransomware-as-a-Service syndicates to abandon financial neutrality in favour of doctrinal support for the Russian state apparatus.

Through a comparative case study applied to the exfiltrated archives (*Conti Leaks* and *Black Basta Leaks*), this thesis has elucidated the mechanism of association through which the Kremlin partially nationalised cybercrime. Benefiting from informal protection guaranteed by Russian security institutions through the *krysha* ("roof") system and from the selective enforcement of the Criminal Code, these cybercriminals became strategic proxies. This outsourcing of aggression enables Russia to project disruptive power against critical infrastructure in Western states, generating a sustained socioeconomic impact.

The complexity of the threat has been structurally amplified through the industrialisation of the intrusion chain. Initial Access Brokers (IABs) have transformed security breaches into a marketable commodity, while underground cryptocurrency-laundering ecosystems ensure the circulation of illicit capital. Furthermore, the adoption of emerging artificial intelligence capabilities is transforming these groups from mere extortionists into actors specialising in psychological subversion and decision-making manipulation. Consequently, the central conclusion of this thesis emphasises that the response to the ransomware threat can no longer be limited to the isolated strengthening of network

security. Dismantling these syndicates requires coherent international cooperation, as well as the application of cyber diplomacy. Medium- and long-term success in an environment characterised by asymmetry and the doctrine of New Generation Warfare will depend on the capacity of global institutions to counter the cybercrime ecosystem.

Therefore, all these arguments and empirical findings confirm the validity of the research direction pursued in this doctoral thesis. The research has demonstrated that the digital landscape can no longer be separated from international kinetic conflicts. The invasion of February 2022 represented a turning point that triggered a profound reconfiguration and ideological fragmentation of the Russian-speaking cybercrime ecosystem, as cybercriminals were recruited, co-opted, or tolerated in order to transform cyber extortion into a state proxy weapon. Accordingly, the thesis concludes that cybersecurity analysis must move beyond traditional technical and criminological boundaries and integrate ransomware into geopolitical studies. Such an approach is necessary to anticipate and neutralise threats that continuously redefine the boundaries of power and national sovereignty in the twenty-first century. The division of ransomware groups into opposing camps supporting the belligerents constituted the central problem identified within this ecosystem, as well as the novel contribution underpinning this thesis. The examination, reading, and interpretation of Russian-language discussions among hackers provided new insights into how these actors collaborate and interact, while the links between members of ransomware groups and the Russian government can no longer be disputed.

The analytical approach adopted in this doctoral thesis was grounded in the premise that the Russian Federation's invasion of Ukraine on 24 February 2022 marked a definitive systemic rupture, necessitating a fundamental reconfiguration of how cybercrime is understood within International Relations. The primary objective of the research was not merely to produce a technical mapping or a chronicle of IT attacks, but to demonstrate a qualitative geopolitical transformation: the conversion of private criminal syndicates into vectors of hybrid warfare, co-opted and instrumentalised by a revisionist state. Through a rigorous empirical investigation of primary data from the *Conti Leaks*, *Black Basta Leaks*, and *The Gentlemen Leaks* archives, the thesis examined the hidden functioning of the "grey zone", demonstrating how the guarantee of impunity provided through the informal *krysha* system strengthened the links between organised crime and the Russian government.

The analysis confirms that contemporary warfare can no longer be conceptualised solely in terms of kinetic battles and land borders. Ransomware has proven to be a highly effective instrument of extortion and strategic targeting below the threshold of a conventional *casus belli*, eroding the classical distinctions under *jus in bello* between civilian and military domains, and between private financial crime and state-directed action.

Looking ahead, the dynamics observed during 2025–2026 indicate that the

ransomware ecosystem will not disappear under international pressure but will continue to evolve towards increasingly dissipative, opaque, and resilient forms. The emergence of highly agile syndicates such as *The Gentlemen*, combined with the proliferation of generative artificial intelligence—from underground models such as *WormGPT* to autonomous strains such as *PromptLock*—marks the beginning of a new era in which technical barriers to entry are declining and the execution speed of asymmetric attacks is increasing exponentially. This technological acceleration will intensify the state of *unpeace* in the digital domain, transforming cyber threats into a persistent feature of global politics.

Ultimately, this doctoral thesis demonstrates that understanding the metamorphosis of ransomware is not merely an academic exercise in decoding the recent past, but an essential analytical framework for deciphering the emerging geopolitical order, increasingly shaped by evolving cybercriminal groups. In an international environment characterised by digital anarchy and competition among major powers, the ability of the international community to understand, expose, and counter this convergence between the underground criminal ecosystem and the state agenda will determine the resilience of the global security architecture in the decades to come.

BIBLIOGRAPHY

Primary sources

Abaimov Stanislav, Martellini Maurizio, *Cyber Arms: Security in Cyberspace*, CRC Press, 2020, 395 pag.

Ackerman Pascal, *Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment*, ed. a II-a, Birmingham, Packt Publishing, 2021, 800 pag.

Aitel Dave, d'Antoine Sophia, Garwin Thomas, Roos Ian, Rostow Nicholas, Sherman Justin, Wagner Abraham, Margin Research, *Russia's Cyber Operations: A Threat to American National Security*, New York, 2022, 119 pag.

Alexandrou Alex, *Cybercrime and Information Technology: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices*, Boca Raton, CRC Press / Taylor & Francis, 2021, 455 pag.

Arquilla John , Ronfeldt David, „Cyberwar is Coming!”, în: *Comparative Strategy*, vol. 12, nr. 2, 1993, pp. 141-165, https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf, accessed in 12.01.2023.

Austin Greg, *Cyber Policy and Economics in an Era of Uncertainty*, London, Routledge, 2014, pp. 45-52.

Bandura Albert, *Moral Disengagement: How People Do Harm and Live with Themselves*, New York, Worth Publishers, 2014, pp. 45-50.

Bandura Albert, *Social Learning Theory*, Englewood Cliffs, Prentice-Hall, 1977, pp. 22-26.

Barker Jessica, *Confident Cyber Security: The essential insights and how to protect from threats*, Londra, Kogan Page, 2023, 265 pag.

Bateman Jon, *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*, Washington, D.C., Carnegie Endowment for International Peace, 2022, 78 pag.

Baylis John, Wirtz James J., Gray Colin S. (editori), *Strategy in the Contemporary World: An Introduction to Strategic Studies* (Sixth Edition), Oxford, Oxford University Press, 2019, 477 pag.

Bodungen Clint, *ChatGPT for Cybersecurity Cookbook: Learn practical generative AI recipes to supercharge your cybersecurity skills*, Birmingham, Packt Publishing, 2023, 372 pag.

Buchanan Ben, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Cambridge, Harvard University Press, 2020, pp. 107-111.

Butler Michael, Wakley Jacob G., *The Business of Hacking: Creating, Developing, and Maintaining an Effective Penetration Testing Team*, Boca Raton, CRC Press, 2024, 311 pag.

Buzan Barry, Wæver Ole, Wilde de Jaap, *Security: A New Framework for Analysis*, Boulder, Lynne Rienner Publishers, 1998, pp. 23-26.

Calder Alan, *The Cyber Security Handbook*, Ely, IT Governance Publishing, 2022, 361 pag.

Caruso Jeffrey, *Inside Cyber Warfare: Mapping the Cyber Underworld*, ed. a III-a, Sebastopol, O'Reilly Media, 2024, 249 pag.

Cyberint, *Israel-Hamas vs. Russia-Ukraine War: Cyber Warfare Insights*, Tel Aviv, Cyberint Technologies, 2024, 35 pag.

Dahj Jean Nestor M., *Mastering Cyber Intelligence: Gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense*, Birmingham, Packt Publishing, 2022, 528 pag.

Dover Robert, Goodman Michael S., Hillebrand Claudia (eds.), *Routledge Companion to Intelligence Studies*, Londra, Routledge, 2013.

Dunn Cavelty Myriam, Wenger Andreas (ed.), *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, Londra, Routledge, 2022, 287 pag.

Edwards Jason, *Mastering Cybersecurity: Strategies, Technologies, and Best Practices*, San Francisco, No Starch Press, 2024, 790 pag.

Erendor Mehmet Emir, *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons*, Wilmington, Vernon Press, 2024, 233 pag.

Galeotti Mark, *Crimintern: How the Kremlin uses Russia's criminal networks in Europe*, Policy Brief, European Council on Foreign Relations (ECFR), 2017.

GitHub, *Conti Ransomware Internal Jabber Chat Logs (DeepL Translated) – File: 185.25.51.173-20210409_en-US.json*, 2022, https://github.com/TheParmak/conti-leaks-englished/blob/master/english_chats/deepl_translated_jabber/2021/185.25.51.173-20210409_en-US.json, accessed in 02.03.2023.

Goșu Armand, *Războiul fără sfârșit: Cum a schimbat invadarea Ucrainei regulile jocului*, Iași, Polirom, 2026, 308 pag.

Graham James, Howard Richard, Olson Ryan (editori), *Cyber Security Essentials*, Boca Raton, CRC Press, 2011, 331 pag.

Gerring, J. (2017). *Case Study Research: Principles and Practices* (2nd ed.). Cambridge University Press.

Greenberg Andy, *Sandworm: A New Era of Cyber War and the Hunt for the Kremlin's Most Dangerous Hackers*, New York, Anchor Books, 2020, 379 pag.

Greenberg Andy, *Traces in the Dark: The Global Hunt for the Dark Web's Cybercriminals*, New York, Doubleday, 2022, 516 pag.

Grimes Roger A., *Ransomware Protection Playbook*, Hoboken, John Wiley & Sons, 2021, 323 pag.

Gritsenko Daria, *The Palgrave HandBook of Digital Russia Studies*, 2021, pp. 115-135,

<https://link.springer.com/book/10.1007/978-3-030-42855-6>, accessed in 04.06.2023.

Gururaj, H. L., V. Janhavi, and V. Ambika, eds. *Social Engineering in Cybersecurity: Threats and Defenses*. Boca Raton: CRC Press, 2024, 241 pp.

Hillebrand, Gregory D., and Bill Ault. *Strategic Cyberspace Operations Primer*. Carlisle: U.S. Army War College, 2023, 221 pp.

Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. *Cybercrime and Digital Forensics: An Introduction*. New York: Routledge, 2022, 813 pp.

Howard, Rick. *Cybersecurity First Principles: A Reboot of Strategy and Tactics*. Hoboken: John Wiley & Sons, 2023, 401 pp.

Janeja, Vandana P. *Data Analytics for Cybersecurity*. Cambridge: Cambridge University Press, 2022, 207 pp.

Jenkinson, Andrew. *Ransomware and Cybercrime*. London: Routledge, 2024, 199 pp.

Inter-American Defense Board. *Cyber Defense Handbook: Guidelines for the Design, Planning, Implementation and Development of a Military Cyber Defense*. Washington, D.C.: Inter-American Defense Board, 2022, 101 pp.

Kaplan, Jacob. *Crime by the Numbers: A Guide to Analyzing and Understanding Publicly Available Crime Data*. Philadelphia: University of Pennsylvania, 2023, 432 pp.

Karmakar, Abhishek. *Certified Blackhat: Methodology to Unethical Hacking*. Chandigarh: White Falcon Publishing, 2019, 135 pp.

Kaspersky. *Common TTPs of Modern Ransomware Groups*. Moscow: Kaspersky Lab, 2023, 137 pp.

KELA. *TELEGRAM: How a Messenger Turned Into a Cybercrime Ecosystem by 2023*. Tel Aviv: KELA, 2023, 59 pp.

Kello, Lucas. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2017, pp. 60–65.

Keohane, Robert O., and Joseph S. Nye. *Power and Interdependence*. 4th ed. Boston: Longman, 2011, pp. 20–25.

Kestner, Peter. *The Art of Cyber Warfare: Strategic and Tactical Approaches for Attack and Defense in the Digital Age*. New York: Springer, 2024, 237 pp.

Kuo, Joshua M., and Ross Gibson. *The Hidden Potential of DNS in Security*. Hoboken: John Wiley & Sons, 2024, 192 pp.

Lefebvre, Henri. *The Production of Space*. Translated by Donald Nicholson-Smith. Oxford: Blackwell Publishing, 1991, pp. 26–33.

Maglaras, Leandros, Ioanna Kantzavelou, and Mohamed Amine Ferrag, eds. *Cyber Security of Critical Infrastructures*. Basel: MDPI, 2023, 318 pp.

Maleh, Yassine, Mamoun Alazab, Loai Tawalbeh, and Imed Romdhani, eds. *Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence*. New York: ACM Books / Morgan & Claypool, 2022, 310 pp.

Martínez, Roberto. *Incident Response with Threat Intelligence*. Birmingham: Packt Publishing, 2024, 468 pp.

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press, 2018, pp. 22–26.

Maurice, Chad, Jeremy Thompson, and William Copeland. *The Foundations of Threat Hunting: Organize and Design Effective Cyber Threat Hunts to Meet Business Needs*. Birmingham: Packt Publishing, 2024, 246 pp.

Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company, 2001, pp. 30–32.

Menzie, Ross. *Hacking for Beginners: Comprehensive Guide on Hacking Websites, Smartphones, Wireless Networks, Conducting Social Engineering, Performing a Penetration Test, and Securing Your Network*. Chennai: Notion Press, 2022, 159 pp.

Millie, Katie. *Cybersecurity Crash Course: Learn Fast, Protect Faster! Don't Be the Next Victim. Secure Your Computers, Smartphones, and Tablets*. Independently published, 2023, 244 pp.

National Research Council. *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. Washington, D.C.: The National Academies Press, 2014, 150 pp.

Nearchou, Nearchos. *Combating Crime on the Dark Web: Learn How to Access the Dark Web Safely and Not Fall Victim to Cybercrime*. Birmingham: Packt Publishing, 2024, 138 pp.

New Strategic Concept. *Clans of Ukraine: Analyzing Links Between Key Groups of the Ukrainian Oligarchy and European and U.S. Families and Institutions*. Bucharest: New Strategic Concept, 2023, 71 pp.

Nye, Joseph S. *Cyber Power*. Harvard University, Belfer Center for Science and International Affairs, 2010, pp. 3–5.

Palacín, Valentina. *Practical Threat Intelligence and Data-Driven Threat Hunting: A Hands-On Guide to Threat Hunting with the ATT&CK™ Framework and Open Source Tools*. Birmingham: Packt Publishing, 2021, 398 pp.

Pease, Andrew. *Threat Hunting with Elastic Stack: Solve Complex Security Challenges with Integrated Prevention, Detection, and Response*. Birmingham: Packt Publishing, 2021, 292 pp.

Prigogine, Ilya, and Isabelle Stengers. *Order Out of Chaos: Man's New Dialogue with Nature*. New York: Bantam Books, 1984, 349 pp.

Rains, Tim. *Cybersecurity Threats, Malware Trends, and Strategies*. 2nd ed. Birmingham: Packt Publishing, 2023, 585 pp.

RAND Europe. *Strategic Competition in the Age of AI*. Cambridge: RAND Corporation, 2024, 144 pp.

Recorded Future. *The Intelligence Handbook: A Roadmap for Building an Intelligence-Led Security Program*. 4th ed. Somerville: Recorded Future, 2022, 198 pp.

Rid, Thomas. *Cyber War Will Not Take Place*. New York: Oxford University Press, 2013, pp.

11–15.

Roddie, Megan, Jason Deyalsingh, and Gary J. Katz. *Practical Threat Detection Engineering: A Hands-On Guide to Planning, Developing, and Validating Detection Capabilities*. Birmingham: Packt Publishing, 2023, 328 pp.

Roy, Kaushik. *Artificial Intelligence, Ethics and the Future of Warfare*. London: Routledge, 2024, 299 pp.

Sandbu, Marius. *Windows Ransomware Detection and Protection*. Birmingham: Packt Publishing, 2021, 290 pp.

Santos, Henrique M. D. *Cybersecurity: A Practical Engineering Approach*. Cham: Springer, 2022, 341 pp.

Schneier, Bruce. *A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back*. New York: W. W. Norton & Company, 2023, 296 pp.

Sharma, Sanjay. *Data Privacy and GDPR Handbook*. Hoboken: John Wiley & Sons, 2022, pp. 5–103. [https://cdn.oujdaibrary.com/books/614/614-data-privacy-and-gdpr-handbook-\(www.tawcer.com\).pdf](https://cdn.oujdaibrary.com/books/614/614-data-privacy-and-gdpr-handbook-(www.tawcer.com).pdf), accessed in April 22, 2023.

Shekokar, Narendra M., Hari Vasudevan, Surya S. Durbha, Antonis Michalas, and Tatwadarshi P. Nagarhalli, eds. *Intelligent Approaches to Cyber Security*. Singapore: Springer, 2026, 210 pp.

Solanki, Shivam R., and Drupad K. Khublani. *Generative Artificial Intelligence: Exploring the Power and Potential of Generative AI*. Boca Raton: CRC Press, 2024, 465 pp.

Soldatov, Andrei, and Irina Borogan. *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*. New York: PublicAffairs, 2015, pp. 210–215.

Spykman, Nicholas J. *America's Strategy in World Politics: The United States and the Balance of Power*. New York: Harcourt, Brace and Company, 1942, p. 41.

Stoddart, Kristan. *Cyberwarfare: Threats to Critical Infrastructure*. London: Palgrave Macmillan, 2022, 586 pp.

Susskind, Jamie. *The Politics of the Future: Digital Technology and Society* [English translation of the Romanian edition title]. Bucharest: Corint Publishing House, 2019, 562 pp.

Sutton, David. *Cybersecurity: The Complete Guide to Cyber Threats and Protection*. 2nd ed. London: BCS, The Chartered Institute for IT, 2023, 340 pp.

Suvorov, Viktor. *Aquarium* [English translation of the Romanian edition title]. Bucharest: Elit Comentator Publishing House, 1993, 352 pp.

Tan, Chang. *Cyberwarfare for Evasive Cyber Tactics*. Singapore: Springer, 2024, 342 pp.

United Nations Office on Drugs and Crime. *Digest of Cyber Organized Crime*. Vienna: United Nations Office on Drugs and Crime, 2021, 144 pp.

Vander Zanden, James W. *Social Psychology*. New York: Random House, 1987, 631 pp. https://archive.org/details/socialpsychology0000unse_h0e1, accessed in April 5, 2024.

Verma, Abhishek, Jitendra Kumar, Hari Mohan Gaur, Vrijendra Singh, and Valentina Emilia

Balas, eds. *Advances in Cyber Security and Intelligent Analytics*. Boca Raton: CRC Press, 2023, 310 pp.

Waltz, Kenneth N. *Theory of International Politics*. Reading, MA: Addison-Wesley Publishing, 1979, pp. 111–114.

Watters, Paul A. *Cybercrime and Cybersecurity*. Boca Raton: CRC Press, 2024, 183 pp.

Wendt, Alexander. *Social Theory of International Politics*. Cambridge: Cambridge University Press, 1999, pp. 1–40.

Wilhoit, Kyle, and Joseph Opacki. *Operationalizing Threat Intelligence: A Guide to Developing and Operationalizing Cyber Threat Intelligence Programs*. Birmingham: Packt Publishing, 2022, 460 pp.

Wittkop, Jeremy. *The Cybersecurity Playbook for Modern Enterprises*. Hoboken: John Wiley & Sons, 2024, 270 pp.

Yin, Robert K. *Case Study Research and Applications: Design and Methods*. 6th ed. SAGE Publications, 2018.

Zimmerman, Carson. *Ten Strategies of a World-Class Cybersecurity Operations Center*. Bedford: MITRE Corporation, 2014, 289 pp.

Zouave, Erik, Marc Bruce, Kajsa Colde, Margarita Jaitner, Ioana Rodhe, and Tommy Gustafsson. *Artificially Intelligent Cyberattacks*. Stockholm: Swedish Defence Research Agency (FOI), 2020, 50 pp.