SOC ACE Serious Organised Crime & Anti-Corruption Evidence Research Programme

Research Paper 22

October 2023

Information Manipulation and Organised Crime

Examining the Nexus

Tena Prelec[1]

1. University of Oxford/University of Rijeka

All correspondence to: tenaprelec@gmail.com

Acknowledgments

This paper has been produced as part of my research fellowship at the Department of Politics and International Relations (DPIR) of the University of Oxford: I would like to thank them for being a wonderful intellectual home during my early post-doctoral years, as well as for their further support through the DPIR Research Fund. I would also like to thank the many experts who have given very useful feedback, guidance and advice at various stages of the genesis of the paper, especially Prof. Heather Marquette, Dr Andi Hoxhaj, as well as staff members within the UK Foreign, Commonwealth & Development Office. I also thank others who gave feedback on earlier drafts, including the participants of the workshop on 'The politics of PR, reputation management and digital influence in the Global South', organised by Dr Corentin Cohen and Prof. Ricardo Soares de Oliveira at the University of Oxford in June 2023. I am grateful to the SOC ACE team for their extensive support and encouragement.

Suggested citation

Dr Tena Prelec is an Assistant Professor at the Centre for Advanced Studies on South Eastern Europe, University of Rijeka. Her research focuses mostly on (anti-)corruption and EU politics, with a geographic focus on the Western Balkans and Eastern Europe more widely. From 2019 to 2023, she has been a Research Fellow (Kleptocracy & Anti-Kleptocracy) at the Department of Politics and International Relations at the University of Oxford. She obtained her PhD from the School of Law, Politics and Sociology, Centre for the Study of Corruption (CSC), at the University of Sussex. Dr Prelec is also a member of the Balkans in Europe Policy Advisory Group (BiEPAG) and a Research Associate at LSEE-Research on South Eastern Europe, London School of Economics and Political Science. Her co-authored book, *Professional Indulgences: British service providers, postcommunist elites, and the enabling of kleptocracy*, is forthcoming with OUP in 2024.

About SOC ACE

The Serious Organised Crime & Anti-Corruption Evidence (SOC ACE) research programme aims to help ‘unlock the black box of political will’ for tackling serious organised crime, illicit finance and transnational corruption through research that informs politically feasible, technically sound interventions and strategies. Funded by the UK’s Foreign, Commonwealth & Development Office (FCDO), SOC ACE is a new component in the Anti-Corruption Evidence (ACE) research programme, alongside Global Integrity ACE and SOAS ACE. SOC ACE is managed by the University of Birmingham, working in collaboration with a number of leading research organisations and through consultation and engagement with key stakeholders.

SOC ACE is funded by the UK Foreign, Commonwealth & Development Office. The views expressed here do not necessarily reflect the UK Government’s official policies.

Find out more

www.socace-research.org.uk

Follow us on X: @SOCACE_research

Follow us on LinkedIn: www.linkedin.com/company/socace-research

SOC ACE | University of Birmingham | Birmingham| B15 2TT | United Kingdom

Contents

Acronyms and abbreviations

CPTED	Crime Prevention Through Environmental Design
DHS	Department of Homeland Security (USA)
DOJ	Department of Justice (USA)
EU	European Union
FBI	Federal Bureau of Investigation
GRU	Main Intelligence Agency (Russian: Glavnoe Razvedyvatel'noe Upravlenie)
IM	Information Manipulation
IMF	International Monetary Fund
OC	Organised Crime
OSINT	Open Source Intelligence
NATO	North Atlantic Treaty Organization
NSA(s)	Non-State Actor(s)
SBU	Security Service of Ukraine

Summary

Information manipulation has been a growing concern in recent years, particularly in relation to the disinformation tactics employed by authoritarian regimes. However, the role of non-state actors, such as organised crime (OC) groups, in information manipulation has been largely overlooked.

This research aims to fill this gap by examining the various ways in which OC groups manipulate information to achieve their objectives and those of actors connected to them. Drawing on Nicholas Barnes' concept of 'political criminality' (2017), this study examines the varying degrees of proximity between criminal actors and the state, which is essential in exploring the complex interplay between OC and information manipulation. Empirical data was collected from several geographies, with a particular focus on Eastern Europe and the post-Soviet space, including Ukraine, Russia, Moldova (Transnistria), and Albania.

The research highlights several dimensions of interest, including: the changing opportunities that technology gives to OC groups to shape facts and narratives; media ownership by organised crime groups and criminal actors; and the ways in which this interplay is situated within the global political economy of offshore finance – including the wider networks of enablers these actors rely on. By shedding light on these aspects, the research seeks to contribute to a more comprehensive understanding of the threat posed by the misuse of information, situates it within the literatures on non-state actors and transnational kleptocracy, and puts forward a framework for analysis that can be tested in future work.

1. Introduction

Information manipulation refers to the intentional and systematic efforts to shape public opinion, attitudes, or behaviour by selectively presenting, distorting, or withholding information (McCornack, 1992). It encompasses various techniques such as disinformation, propaganda, spin, and censorship, as well as the manipulation of images or statistics. While often associated with negative connotations, information manipulation is a broader and more subtle term than propaganda (Auerbach & Castronovo, 2013).

Organised crime (OC) typically refers to groups or networks engaged in criminal activities, including cybercrime and hacking. While hacking groups may or may not be classified explicitly as criminal organisations, they are included within the scope of OC due to their involvement in illicit activities such as cyberattacks, data theft, and disruption of critical systems. Although OC is commonly perceived as ideologically neutral, this research explores the potential nexus between OC and information manipulation and examines its various manifestations.

The research serves a dual purpose. Firstly, it presents a series of case studies that exemplify different aspects of the OC-information manipulation nexus. These case studies provide empirical evidence and shed light on the interplay between OC and information manipulation. Secondly, it proposes a theoretical framework to facilitate the examination of this nexus, drawing on the refined OC-terror nexus framework by Makarenko and Mesquita (2014) and – most importantly – on Barnes' framework of 'political criminality' (2017).

To establish the groundwork for the research, the literature review explores relevant topics such as non-state actors (NSA) and the interaction between OC and terrorist groups. It also investigates the interconnectedness between politics and OC, emphasising the growing convergence between these spheres. By highlighting the increasing interaction between politics and OC, the research establishes the significance of examining the OC-information manipulation nexus.

The structure of the paper is as follows. First, the literature review sets the stage by exploring relevant literature on NSAs, the OC-NSA nexus, and the agents involved in information manipulation. Next, a conceptual framework is advanced, building upon the refined OC-terror nexus and the concept of political criminality. This framework provides a conceptual lens for analysing the relationship between OC and information manipulation. Subsequently, case studies are presented and analysed to examine the empirical manifestations of the OC-information manipulation nexus. Finally, the conclusion elaborates the theoretical framework, summarising the key findings and highlighting avenues for further research.

2. Shedding light on uncharted territory: a critical analysis of existing literature

The nexus between organised crime and disinformation has received very limited attention in the existing literature. As this relationship represents a wholly novel research angle, this research aims to fill this gap by situating it within the broader context of non-state actors, illicit finance, and transnational kleptocracy. The literature review follows a four-step approach to achieve this objective. Firstly, it examines the literature on non-state actors, exploring their characteristics and roles. Secondly, it investigates the connection between organised crime and other actors, particularly terrorist organisations, which have often been researched in conjunction with organised crime groups. Then it looks at the flipside, identifying the actors involved in information manipulation. Lastly, it delves into the existing research pertaining to the intersection of organised crime and disinformation.

2.1. Why non-state actors matter

Non-state actors (NSAs) have historically received inadequate attention in the field of international relations and politics. While they were often perceived as insignificant to political processes, this notion has been debunked. Josselin and Wallace (2001) redefine the concept of NSAs beyond the traditional understanding of non-governmental organisations (NGOs), encompassing a diverse range of actors such as civil society organisations and also churches, transnational political parties, as well as economic and criminal actors. They argue that the realm of NSAs is multifaceted, involving public-private partnerships and exhibiting various shades and intermediate connections. It should also be acknowledged that violent actors are part of this complex landscape (Dutka, 2006).

The significance of NSAs and the norms they espouse is also evident in their pursuit of self-determination. While international law generally prioritises territorial integrity over self-determination, sub-state actors aligned with the values of dominant powers receive special consideration. Sometimes, such NSAs can literally make or break a state, as illustrated by Anne Gardner's (2011) analysis of cases such as Kosovo, Nagorno-Karabakh, and Western Sahara. In Kosovo, for example, the advocates of self-determination found fertile ground for their cause after a decade of Belgrade-instigated wars in the region. With the Kosovo Liberation Army as their military arm, they garnered support from Western powers, which backed Kosovo's plight and its unilateral declaration of independence from Serbia. On the other hand, the struggle of the Polisario Front in Western Sahara has not received as much international attention, resulting in a territory that is still highly disputed, with the United States backing Morocco’s sovereignty over it.

Regarding OC groups as NSAs closely connected to the state, Alina Rocha Menocal (2022) asserts that OC groups should be considered integral components in the analysis of political settlements and elite bargains.[1] This is due to the fact that OC group members themselves can wield significant economic and political influence, interacting with, and sometimes even becoming part of, other important actors within the state and society. These interactions, which include government authorities, politicians, business elites, and non-state armed groups, shape the 'rules of the game' (Rocha Menocal, 2022).

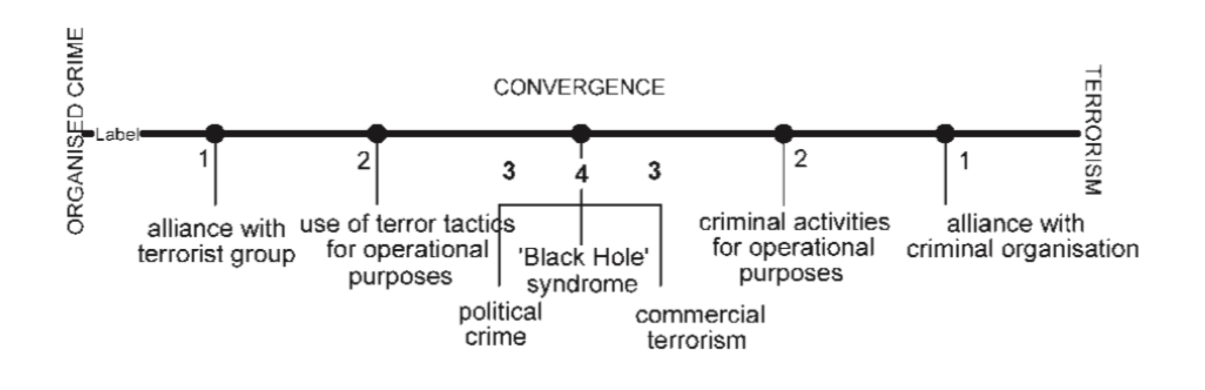
NSAs are therefore involved in shaping our politics, both domestically and internationally. This is also the case with money and reputation laundering, through the phenomenon of transnational kleptocracy. Heathershaw et al. (forthcoming, 2024) examine the relationship between elites and their enablers, arguing that these dynamics have not been adequately addressed in the field of international relations. It has been demonstrated that the collaboration between elites and enablers has successfully circumvented anti-money laundering (AML) regulations, suppressed critics, undermined the rule of law, and even facilitated foreign interference in political processes. The primary actors driving these processes are not states or international institutions, although they are often co-opted and utilised to these ends. Instead, it is the elites and their enablers who take centre stage. This highlights the necessity of being more attuned to examining networks of NSAs, scrutinising everyday power relations as they take place across borders.

2.2. The OC-terrorism nexus

The study of OC in conjunction with other NSAs has mostly focused on their link with terrorist groups. Traditionally, OC and terrorist entities were examined independently, but this approach underwent a significant shift following the events of 9/11. The US-led crackdown on sources of terrorist funding has pushed those groups to look for monetary resources in what is more the domain of OC groups. The two, therefore, started to find more points of contact in their activities. This phenomenon found reflection in the literature, with some arguing that terror groups were transforming into hybrid criminal-terror entities (Sanderson, 2004). In particular, Tamara Makarenko's characterisation of the crime-state nexus as a 'continuum' between which groups can slide has been very influential. In her 2004 paper, she posits that OC and terrorist groups exist on the same plane and are capable of converging at a central point: a 'black hole' syndrome characterised by either extremely weak government control or civil war in which the two are brought closest to each other (Figure 1). Substantiation of this blurring of the lines between terror and OC groups in unstable environments has been brought forward in cases such as Kosovo and Chechnya (Šmid, 2014). Drug trafficking often provided the main financial link.

[1] Defined as follows (Rocha Menocal, 2022, p. 2): 'political settlements constitute a common understanding or agreement, principally among elites, on the balance and distribution of power, allocation of resources and wealth, and on the rules of political engagement that leads to a significant reduction in anti-systemic violence and other forms of disruption. Elite bargains, which tend to focus on agency, leadership and the choices leaders make, can be understood as discrete agreements that explicitly set out to renegotiate the distribution of power and allocation of resources between elites, cumulatively shaping and changing the overarching political settlement.'

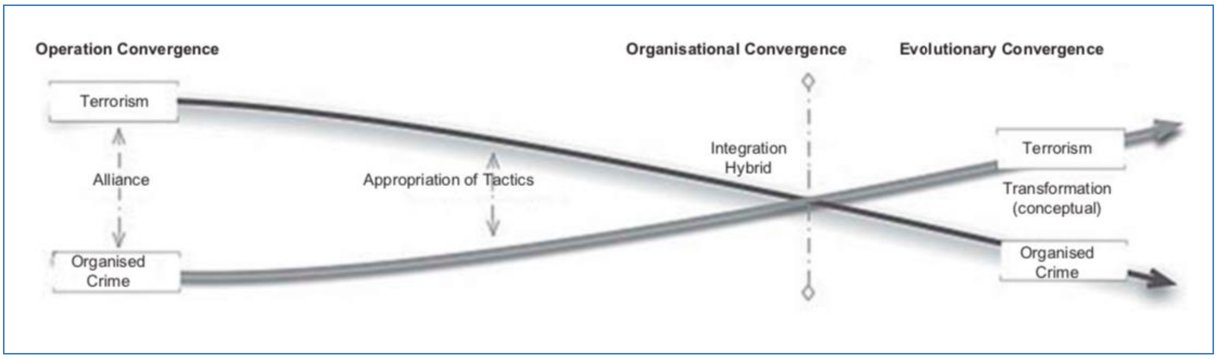
Figure 1. The crime-terror continuum by Makarenko (2004, p. 4)


ORGANISED CRIME
Label
CONVERGENCE
TERRORISM
1
alliance with terrorist group
2
use of terror tactics for operational purposes
3
4
3
'Black Hole' syndrome
political crime
commercial terrorism
2
criminal activities for operational purposes
1
alliance with criminal organisation

Others have warned, however, that terrorist and OC groups should not be conflated, as their motives and ways of operating are fundamentally different. Hutchinson and O'Malley (2007) find that the two sometimes cooperate insofar as terrorist groups need financing to implement their activities, but while terrorist groups have an ideological agenda and therefore seek the attention of the media, OC groups, by and large, shun the limelight. In examining their nexus, they find that the most likely relationship is a *temporary* one, via one-time contracts for quick profit. A more enduring relationship is a *parasitic* one, where terrorists feed off OC activities. Here, too, the relationship lasts only as long as the two remain useful for each other and their ideological differences do not collide. They find no evidence of *symbiotic* relationships, in which the two would collaborate closely and for the long haul, which they explain with the lack of political/ideological alignment. Most often, they find that terrorist groups rely on 'in-house' operators to secure funds for their activities, rather than striking alliances with OC (Hutchinson & O'Malley, 2007, p. 1104).

Makarenko herself refined her original framework on a few occasions. Researching this nexus in relation to European countries, Makarenko and Mesquita (2014) made a clearer distinction between the paths of the two types of groups. They propose a dual framework consisting of an organisational plane and an evolutionary plane. On the organisational plane, the authors observe the adoption of techniques by each group from the other. For instance, terrorist organisations may adopt OC methods as a means of generating financial resources. Similarly, OC groups may employ terrorist techniques for political or operational purposes, as evidenced in cases such as Italy, the Balkans, and the Caucasus during the 1990s. On the evolutionary plane, the authors explore the phenomenon of groups converging into one another. A notable example is the Fuerzas Armadas Revolucionares de Colombia (FARC), where an OC group begins to utilise political or ideological rhetoric as a disguise or front for engaging in organised crime activities. They note that hybrid entities are a rare phenomenon in mature democracies, but there are examples such as the Irish Republican Army (IRA), whose offshoots maintained a rhetorical political stance, while focusing on perpetuating criminal activities and thus becoming 'full-time criminals and part-time terrorists' (Makarenko & Mesquita, 2014, pp. 260-261).

Figure 2. Refined OC-terrorism nexus model by Makarenko and Mesquita (2014)



A shared finding that emerges from the review of the literature on the terror-OC nexus, and one that is very relevant to the subject at hand, is that the main difference between terrorist and OC groups lies in the lack of an ideological/political purpose in the case of OC groups. Their first and foremost aim is that of making money through (mostly) illicit means. In their pure form, OC groups are therefore devoid of ideology and thus of a message to propagate. If their link with information manipulation is to be established, it therefore needs an added layer.

2.3. Information manipulators

Who are the agents behind information manipulation? From the discussion above it will not come as a surprise that social science literature has largely ignored a possible connection between OC and information manipulation. After all, the lack of a message to push does not provide enough of a motivation for OC groups to engage in the difficult and time-consuming business of shaping hearts and minds. And yet, this overlooks a clear trend: the increasing points of contact between OC and politics. The growing influence of transnational organised crime in the political process within states and on the international level has been squarely recognised (Paraschiv, 2013).

The primary actors who stand to benefit the most from information manipulation are undoubtedly those involved in the political arena, whether at the domestic or international level. Consequently, existing research has predominantly focused on the use of information manipulation by governments and political actors. Scholars specialising in authoritarianism have extensively explored how governments manipulate narratives and facts to control public opinion and suppress dissent, thereby hindering collective action by citizens (Chen & Xu, 2017; Edmond, 2013). Within the field of political psychology, it has been argued that the objective of information manipulation by authoritarian regimes is not necessarily to disseminate outright falsehoods or deceive citizens into believing them. Rather, it aims to induce a state of apathy and demobilisation among the populace, instilling a sense of scepticism and relativism towards all information, with the intention that citizens become less inclined to take action against their regime, as they are unable to form consistent opinions (Alyukov, 2022).

Non-academic works have echoed these findings, exemplified by the depiction of contemporary Russia as a post-modern society, lacking a unifying ideology and characterised by a climate where ‘nothing is true and everything is possible’

(Pomerantsev, 2014). This environment becomes fertile ground for susceptibility to disinformation. As globalisation has advanced, authoritarian rulers have increasingly transnationalised their repressive practices (Schenkkan et al., 2020), including information manipulation. Far from being a localised issue, the manipulation of facts and narratives has now become a transnational problem, akin to money laundering and reputation laundering (Heathershaw et al., 2018; Heathershaw et al., 2021), with which it shares a mutually reinforcing relationship.

2.4. OC-information manipulation points of contact

Despite the existence of a substantial and growing body of literature on information manipulation, the specific link between information manipulation and NSAs, and particularly OC, has not been studied systematically. However, there are works that have examined certain points of contact between the two.

During the Cold War, there were documented instances of governments collaborating with NSAs in information manipulation efforts. Pacepa and Rychlak (2013) reveal how the Soviet Union deployed thousands of spies in the Muslim world to fuel political unrest against the United States and Israel. They also argue that the KGB conducted disinformation campaigns during the Vietnam War to sow conflict among American citizens, and that disinformation was employed in conspiracy theories surrounding the assassination of John F. Kennedy. Information manipulation tactics were not exclusive to the communist bloc; the CIA's strategic use of modern art to shape narratives and win hearts and minds in the Soviet Union (Stonor Saunders, 1995)[2] exemplifies how both sides in the Cold War recognised the importance of working with non-state actors to advance their objectives.

In more recent times, some attention has been directed towards the impact of new technologies on illicit finance and illegal trade (Shelley, 2018; Bartlett, 2016). However, these works often lack a comprehensive examination of the networks of actors operating within these spaces and their methods. Consequently, our understanding of the relationship between NSAs involved in information manipulation and the state remains limited. In particular, the impact of modern technologies and globalisation on the ability of OC groups to adapt and manipulate information has not received sufficient attention, warranting further investigation.

The literature review reveals several key points. Firstly, political actors are the primary agents interested in information manipulation. Therefore, understanding the relationship between OC groups and politics becomes crucial in comprehending the motives behind OC engagement in information manipulation. Secondly, due to the rapid evolution of communication methodologies, both the methods and the intensity of information manipulation activities, including those involving OC, are expected to be dynamic and subject to change. Thirdly, information manipulation aims to undermine and confuse the public rather than solely relying on outright propaganda. It seeks to

[2] Initially considered a rumour, it was later confirmed as fact: the US Central Intelligence Agency fostered and promoted American Abstract Expressionism, using unwitting artists such as Pollock and Rothko in a 'cultural Cold War' (Stonor Saunders, 1995).

muddy the waters and create uncertainty. Furthermore, while the evidence of interaction between OC and information manipulation remains limited, Eastern Europe, particularly the post-Soviet space, has been highlighted as the region where this nexus is most apparent. Therefore, this region will be the focus of our search for possible evidence. With these insights in mind, the next step is to develop a theoretical framework that can effectively accommodate the emerging study of the relationship between OC and information manipulation.

3. Conceptual framework: understanding the organised crime-information manipulation nexus

The particular domain of the intersection of OC and information manipulation raises questions in regard to the level of entanglement of OC with the state. The manipulation of narratives primarily serves political agendas, and in many countries, the state actively combats organised crime. However, in certain cases, the relationship becomes more complex. As famously noted by Sicilian magistrate Paolo Borsellino, in Italy, 'politics and mafia are two systems of power contending the control of the same territory: they are either at war with each other or come to an agreement' (Abbate & Gomez, 2007, p. 36). Moreover, there are countries where the lines between OC and the state become blurred, where they exist in a symbiotic relationship. Individuals in positions of power often either co-opt or are co-opted by organised crime networks. This intricate dynamic raises important considerations for understanding the nexus between OC and information manipulation.

To account for these issues, this evidence review adopts insights from a framework developed by Nicholas Barnes (2017). While OC groups do not seek to replace the state or become part of the official administrative apparatus, Barnes notes that they have 'increasingly engaged in the politics of the state… [by developing] variously collaborative and competitive relationships with the state' (Barnes, 2017, p. 967). He thus argues that organised crime should be incorporated within the political violence literature, and suggests four dimensions to distinguish different levels of crime-state engagement. In this conceptualisation, they vary from confrontation (foreseeing high competition between OC groups and the state), enforcement-evasion (low competition), alliance (low collaboration) and integration (high collaboration). The following table summarises the implications of these dimensions for the OC-IM (Organised Crime-Information Manipulation) nexus, distinguishing between them based on competition and collaboration.

Table 1: Hypotheses for OC and information manipulation by crime-state arrangement

Crime-state nexus (after Barnes, 2017)	Implications for the OC-IM nexus (hypotheses)
Confrontation (high competition)	In cases of state-OC competition, OC groups are expected to either: refrain from engaging in IM or, if they do engage, manipulate information to the detriment of the state.
Enforcement-evasion (low competition)	
Alliance (low collaboration)	In case of state-OC collaboration, OC groups are expected to manipulate information in a manner that serves the state, either ad hoc or systematically.
Integration (high collaboration)	

Before proceeding to analyse empirical case studies and test the framework outlined above, it is important to consider a few additional insights. First, actors may move across the spectrum of crime-state arrangements, suggesting that the categorisation should be flexible rather than strict. Second, the above-mentioned framework proposed by Makarenko and Mesquita (2014) regarding OC and terrorism is already included in the discussed framework as far as the evolutionary plane is concerned (because the convergence of groups into each other is reflected in the gradation from confrontation to integration). However, their organisational plane prompts us to examine the mutual use of tactics between the groups. Finally, when examining the link between OC groups and state actors in information manipulation, it is essential to consider not only the quality but also the quantity or intensity of the information manipulation actions. Therefore, the conceptual framework applied to the case studies will consider two dimensions: integration (aligned with the crime-state nexus) and intensity (the potentially varying intensity of information manipulation activities). Represented visually in a table, the Y axis (vertical) will therefore take into account OC's integration with the state, while the X axis (horizontal will consider the intensity of the IM activity.

Table 2: The Organised Crime (OC)-Information Manipulation (IM) nexus

OC-IM Nexus				
Integration				
Alliance				
Enforcement-evasion				
Confrontation				
Integration (column)/ Intensity (row)	**Low**	**Moderate**	**High**	**Very high**

Following the conceptual framework presented, the analysis in this research paper adopts a two-dimensional approach to examine the link between OC groups and state-connected actors in information manipulation. The framework considers the dimensions of integration and intensity to understand the dynamics and patterns of this nexus.

In terms of integration, the focus is on the alignment between OC groups and the state, ranging from confrontation to integration. The Y axis of the framework represents this continuum of integration, with varying degrees of collaboration or alignment between OC and state actors. This dimension helps identify the level of cooperation, shared interests, or interdependence between the two entities.

Regarding intensity, the framework recognises that information manipulation activities can vary in their magnitude or extent. The X axis represents the intensity of information manipulation (IM) activity, encompassing techniques such as disinformation, propaganda, censorship, and selective presentation of facts. This dimension allows for an assessment of the scale and impact of IM activities employed by OC groups and their collaboration with state actors.

By plotting the empirical case studies within this conceptual framework, we aim to understand how different OC groups and state actors engage in information manipulation, considering both their level of integration and the intensity of their IM activities. The placement of each case study within the framework is determined based on an analysis of relevant factors such as the nature of the relationship between OC and state actors, the extent of information manipulation tactics employed, and the overall dynamics observed.

It is important to note that the categorisation within this framework is not intended to be rigid, as actors may transition across different points on the integration spectrum. This flexible approach allows for a comprehensive analysis of the complex interactions between OC groups and state actors in the context of information manipulation.

Through this approach, the research aims to provide insights into the patterns, trends, and dynamics of the OC-information manipulation nexus in each of the case studies examined in the following section, thus shedding light on the relationship between these actors, and their strategies in shaping public opinion and influencing societal outcomes.

4. Empirical analysis: case studies

The choice of case studies is based on both methodological and practical considerations. As highlighted in the discussion above, Russia and the post-Soviet space provide numerous examples where points of contact between OC and information manipulation have been explored in existing research. Additionally, considering the limited scope and timeframe of this review, focusing on five Eastern European cases is a reasonable and well-sampled approach, given the researcher's linguistic abilities and geographic expertise.

In what follows, five case studies are presented to delve into the dynamics of the OC-information manipulation nexus. They explore the following areas: 1) the intersection of cybercrime and the Russian state; 2) the role of Evgeny Prigozhin, an OC-linked oligarch, in carrying out information manipulation on behalf of Russia; 3) media ownership in Transnistria, exemplifying how OC can influence and control politics; 4) media ownership in Russia, illustrating how politics can shape OC-linked media outlets; and 5) media ownership in Albania, showcasing the interplay and symbiotic relationship between OC and the state.

4.1. Cybercrime: Russia’s invasion of Ukraine

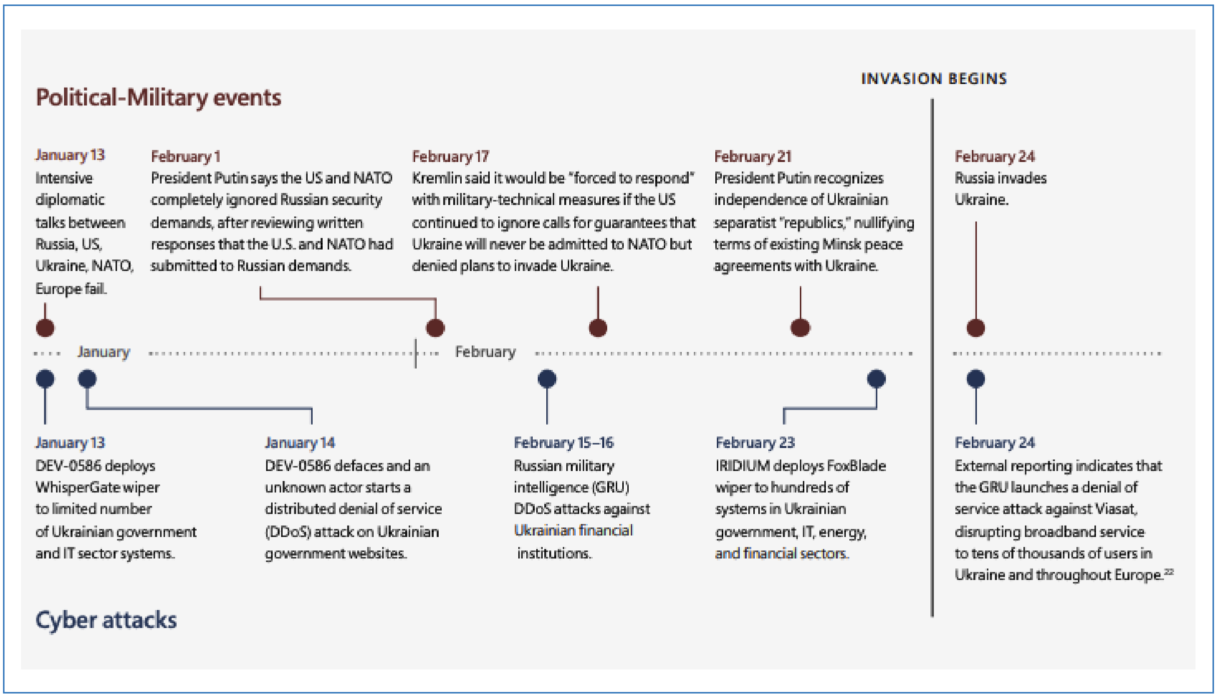
This case study looks at Russia's use of cybercrime groups in the context of the war in Ukraine. Russia's deployment of cyber criminals and hacktivists in Ukraine is not random; instead, it is a result of the country's intelligence, military, and law enforcement services utilising their longstanding connections with criminal hackers to support their war efforts. As will be demonstrated from the examples below, however, their links with the Kremlin vary.

4.1.1. State-sponsored hacking

In a report published in April 2022, Microsoft's Threat Intelligence Center (MSTIC) analysed the tactics, techniques, and procedures used by Russian state-sponsored hacking groups to target Ukrainian government entities, critical infrastructure, and individuals (Microsoft Digital Security Unit, 2022). According to this study, the Russian government has been conducting a persistent and sophisticated cyber campaign against Ukraine since 2014. From then to 2022, the attacks increased in frequency and complexity, and the scope of targets expanded beyond government and military entities to include the private sector and civil society.

The report identifies several Russian state-sponsored hacking groups responsible for the attacks. These groups have used a range of techniques, such as phishing, malware, and supply chain attacks, to gain access to targeted networks and steal sensitive information. The attacks have disrupted critical infrastructure, including power grids and transportation systems, and have caused significant financial losses for Ukrainian businesses.

Figure 3: Timeline of Russia's political-military activities in Ukraine between January and February 2022



January 13
Intensive diplomatic talks between Russia, US, Ukraine, NATO, Europe fail.

February 1
President Putin says the US and NATO completely ignored Russian security demands, after reviewing written responses that the U.S. and NATO had submitted to Russian demands.

February 17
Kremlin said it would be "forced to respond" with military-technical measures if the US continued to ignore calls for guarantees that Ukraine will never be admitted to NATO but denied plans to invade Ukraine.

February 21
President Putin recognizes independence of Ukrainian separatist "republics," nullifying terms of existing Minsk peace agreements with Ukraine.

February 24
Russia invades Ukraine.

January 13
DEV-0586 deploys WhisperGate wiper to limited number of Ukrainian government and IT sector systems.

January 14
DEV-0586 defaces and an unknown actor starts a distributed denial of service (DDoS) attack on Ukrainian government websites.

February 15–16
Russian military intelligence (GRU) DDoS attacks against Ukrainian financial institutions.

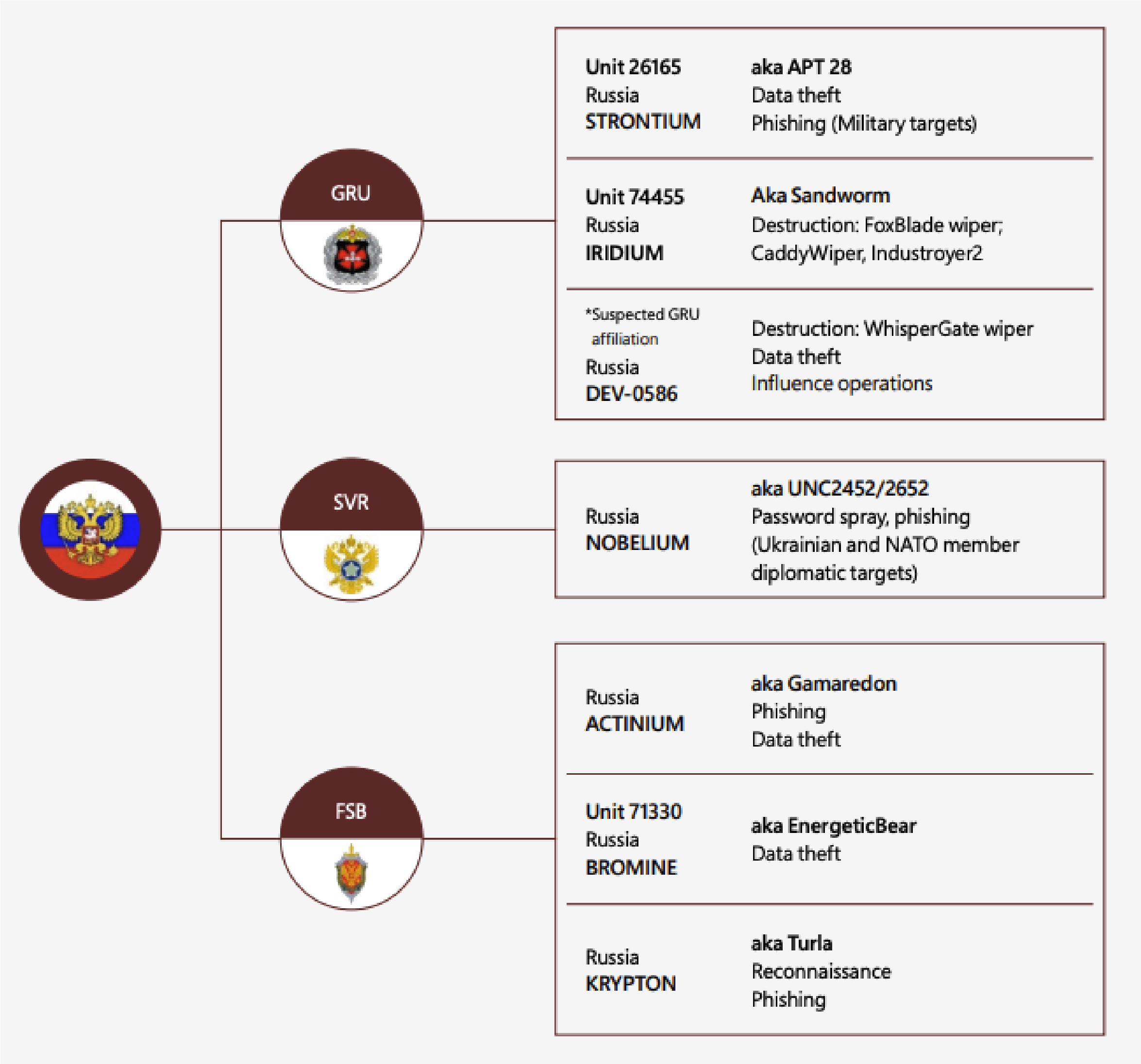
February 23
IRIDIUM deploys FoxBlade wiper to hundreds of systems in Ukrainian government, IT, energy, and financial sectors.

February 24
External reporting indicates that the GRU launches a denial of service attack against Viasat, disrupting broadband service to tens of thousands of users in Ukraine and throughout Europe.[22]

Source: Microsoft Digital Security Unit (2022).

The Microsoft report also clearly lays out the connections of the cybercrime groups involved in malicious activity against Ukraine and their linkages with the various branches of the Russian security services. As illustrated in Figure 4 below, the Main Intelligence Directorate (GRU) – the foreign military intelligence arm of the Russian Armed Forces – has direct connections with the units named Strontium and Iridium, and suspected connections with DEV-0586. The Foreign Intelligence Service (SVR) controls Nobelium, while the Federal Security Service (FSB) has links to Actinium, Bromine and Krypton. While it is difficult to identify the moment when long-term espionage shifted to direct support of the invasion, the report assesses that these Russia-aligned groups were pre-positioning for conflict as early as March 2021, when they also started conducting operations against countries that are located outside Ukraine.

Figure 4: Cybercrime groups active in Ukraine and their connections to Russia's intelligence services



Source: Microsoft Digital Security Unit, 2022

In laying out the increasingly aggressive and frequent cyberattacks conducted by Russia in the pre-invasion period, the report notes that 'Russian threat actors launched increasingly disruptive and visible cyberattacks against Ukraine on the heels of major diplomatic failures related to the conflict' (Microsoft Digital Security Unit, 2022, p. 7). This is consistent with the findings of Owen et al. (2022), who, in their study on Russian foreign policy and illicit financial flows, have observed the escalatory nature of the actions of Russia-connected actors. When Russia does not achieve its aims in a more conciliatory way, it tends to escalate from soft power, to more direct political influencing, and to outright violence.

4.1.2. From rogue actors to state-co-opted cybercrime

The more clearly state-sponsored groups, as discussed above, are only the tip of the iceberg. A cyber threat analysis published in early 2023 (Insikt Group, 2023) raises two main points. First: some criminal organisations and hacktivist groups (including Conti, Killnet and Xaknet) have openly pledged allegiance to the Russian state; they have been thwarting attacks on Russian entities and infrastructure and sabotaging Ukrainian networks. Second: other malware hackers, such as DarkCrystal RAT, Colibri Loader, and WarZoneRAT, are being used as proxies by Russian state hackers to target networks in Ukraine and its allies, such as the United States, United Kingdom, other NATO members, and Japan. These actors allow the Kremlin to deny allegations of state-sponsored attacks on Western firms and infrastructure.

The findings of the 2023 report build on in-depth analysis carried out by the same analysts in 2021 (Insikt Group, 2021) that showed it is highly probable that Russian intelligence, military, and law enforcement services have had a longstanding and unspoken agreement with seemingly ‘scattered’ cybercriminal threat actors. In some cases, it is almost certain that these agencies have maintained systematic relationships with cyber criminals, either through indirect collaboration or recruitment. The report documents a series of direct links, including with former FSB employee Major Dmitry Dokuchaev, indicted by the U.S. Department of Justice for conducting a data theft operation targeting Yahoo in 2014 that sought to acquire information to be utilised in espionage operations benefiting the Russian government.

An interesting example of this long-standing collaboration and of the strengthening cybercrime-Kremlin ties in the context of the war in Ukraine is the notorious cyber criminal group Conti. As a sophisticated business and not unlike many Silicon Valley tech companies (for example, with clearly defined recruiting procedures and a set hierarchical structure), Conti is known for deploying ransomware attacks against organisations worldwide, with a focus on high-value targets such as corporations, healthcare providers, and government agencies. It often uses double extortion tactics, stealing sensitive data from their victims and threatening to publish them if the ransom is not paid. The group has been active since at least 2020 and, while it is believed to be based in Russia, it has counted members from a wider range of countries. Their political allegiances were mixed at best. But on 25 February 2022, Conti issued a statement aligning themselves with the Kremlin – causing a former Conti member, hailing from Ukraine, to leave the group and leak a large amount of chat logs that throw light on the internal functioning of the group and lay bare the ties that senior Conti operatives kept with the FSB.

Analysing this data, Nershi and Grossman (2022) show that the Russian government maintains loose ties with ransomware groups such as Conti. They argue that those groups operate as independent criminal organisations but occasionally perform favours for the government, which, in exchange, provides them with safe harbour from prosecution. Furthermore, based on a dataset of over 4,000 victims of ransomware attacks located across 102 countries between May 2019 and May 2022, they find an increase in the average number of attacks by Russia-based groups in the months before an election across six democratic countries. By comparing the victims of Russia-based groups with those based outside Russia, Nershi and Grossman (2022) were able to ascertain that the behaviour of Russia-based ransomware groups was consistent with Russian political goals.

In parallel, cyberattacks on other countries by Russian groups have also intensified. In the UK, a January 2023 ransomware attack by Russian crime gang LockBit against the Royal Mail – which is categorised as critical infrastructure by the UK government – has raised concerns as to whether they were acting under state orders (Espiner & Tidy, 2023). Like Conti, LockBit also operates a sophisticated business, with clear organisational structures, skills specialisation and even public relations resources. The advent of the cryptocurrency industry has bolstered these groups, as its illegal elements provide the financial infrastructure for ransom payments (Kumar & Fowler, 2023).

4.1.3. The response

The increase in cybercrime has not gone unnoticed. International organisations have thus offered technical expertise to counter Russian disinformation, with the European Union deploying its Cyber Rapid Response Team to help Ukraine detect and mitigate cyber threats, while NATO has increased information sharing about Russian cyberattacks. Private companies have also aided in mitigating the spread of false content, and reinforced cybersecurity. The G7 Rapid Response Mechanism was used to reach partners who suffer from Russian disinformation, including Ukraine and Moldova, aiming to bolster their cyber resilience and counter disinformation (OECD, 2022).

4.1.4. The tightening linkages between cybercrime groups and Russia

Be it because of ideology or outright pragmatism, the politicisation of cybercrime groups by the Russian state – and its increase in the context of the war in Ukraine – is an unambiguous trend that emerges from the evidence examined in this section. Some groups have clearly established links with the Russian state's structures, mainly through the secret services. Others have been operating as individual actors, but their links with state structures have been increasing.

Some groups, like Conti, have made an open show of their allegiance to the Russian cause since the invasion of Ukraine started. It may be that these and other hackers have little choice but to comply with the Kremlin's demands: if they go against the Kremlin's policies, calculations, or instructions, they may be seen as disposable, as evidenced by Russia's crackdown on REvil and other cyber gangs in 2021, when the FSB raided 25 addresses and arrested 14 hackers, seizing more than 426 million roubles' (£4.6 million) worth of cash, cryptocurrency, computers, and cars (Deutsche Welle, 2022).

It is also likely that financially motivated cyber actors who are exploiting geopolitical instability are assisting the Russian state's interests, either knowingly or inadvertently. A much less sophisticated example of this interaction is provided by the youngsters in North Macedonia writing clickbait with fake news that served the Kremlin's agenda during the 2016 US elections. Researchers identified an autodidact social media expert, teacher, and mentor to local fake news operators as the epicentre of this phenomenon, stressing the financial component of the (surprisingly successful) operation (Hughes & Weismel-Manor, 2021).

Strategically, cybercrime groups are useful tools because they enable the Kremlin to claim plausible deniability. This allows Moscow to hide itself behind them, or to leave the benefit of the doubt as to who has carried out the attacks and with what aims. These dynamics are consistent with the wider modus operandi of Russia's information manipulation, which functions through a game of smoke and mirrors, aiming not so much at establishing a new truth, as much as to undermine truth itself.

4.2. Bot adhocracy: Evgeny Prigozhin

The activities of Evgeny Prigozhin, who was initially known as 'Putin's cook' due to the many restaurants and hospitality ventures he owned in St Petersburg, illustrate an example of what has been referred to as 'adhocracy' (Galeotti, 2020): a system in which wealthy individuals receive benefits from the Kremlin in exchange for their loyalty in executing specific tasks. As it will be shown, it is also a case in which the ties between oligarchy and organised crime are evident. Adhocracy, rather than a micro-managed process, is a system in which the 'boss' (in this case, Putin) 'sets broad objectives and hints at what kinds of things he would like to see… [which] generates flexibility and initiative, but at the cost of duplication and control' (Galeotti, 2020). The spheres in which Prigozhin offered his services were various. He was infamous for being the head of the Wagner mercenary group, which has supported Russia's military activity in places like Syria, Sudan, and Ukraine – with increasing intensity. The connections with the Russian state are manifest. In June 2023, after Prigozhin's aborted mutiny,[3] Vladimir Putin admitted that the Kremlin had been funding the paramilitary group from the state budget, revealing that Wagner received over 86 billion roubles (around £740 million) from May 2022 to May 2023 alone (Camut, 2023). It would appear, however, that the disobedience did not go unpunished, as Prigozhin was on the private plane that crashed outside Moscow in late August 2023, with no reported survivors (Mpoke Bigg, 2023).

However, Prigozhin also took a large role in the remit of information manipulation, including election meddling. Prigozhin's rise to media prominence was a consequence of the anti-Putin protests that followed the 2012 presidential elections, widely seen as rigged (OSCE, 2012; Parfitt, 2012). On that occasion, the state-controlled media outlets failed to penetrate the social media sphere that was used by the protest movement to coordinate their actions. Prigozhin offered a straightforward solution: hiring hundreds of young people and having them write pro-Putin comments. In 2013, Novaya Gazeta revealed that Evgeny Prigozhin was the owner of the Internet Research Agency (Garmazhapova, 2013). The organisation was responsible for publishing propaganda and loyalist comments, and had specialised departments for creating social media posts, news, videos, and foreign press website comments. Novaya Gazeta reported that the company provided ideological training and lectures, and conducted proficiency tests. Employees were paid to write comments that praised President Putin's achievements, denounced opposition activities, and endorsed the state-sanctioned views of the Syrian and Ukrainian conflicts.

The Internet Research Agency (widely known as the 'troll factory') was located in Olgino near St Petersburg and had a staff of about 400 people who worked almost around the clock. Retired police colonel Mikhail Bystrov was believed to be the founder and general

[3] On 23 June 2023, Prigozhin led a rebellion against the Russian military establishment. He took control of Rostov-on-Don the next day and instructed the Wagner mercenaries to march towards Moscow, in effect threatening to tip the country into civil war, but turned his tanks back as they came within 200km of the Russian capital.

director of the agency. Maria Kuprashevich, an employee of the PR department in Yevgeny Prigozhin's company Concord Management and Consulting, was also linked to the agency. The agency's monthly budget was at least 20 million roubles. In 2014, the hacker group Anonymous International confirmed that the agency was funded by Evgeny Prigozhin through his financial structures and published related documents. The Federal News Agency (FAN) grew out of the troll factory and shared the same St Petersburg residence address, funding source, and leadership. By 2017, FAN consisted of 16 news sites, employed 250 people, and had a monthly audience of up to 36 million people. (Investigations about the troll factory were published by Novaya Gazeta, The New York Times Magazine, Fontanka.ru, RBC, and MR7.ru.)

Prigozhin later branched out of social media, entering the mainstream media scene, too. While the Internet Research Agency was eventually closed, Prigozhin became the head of the Board of Trustees of the Patriot Media Group in 2019 (OpenMedia, 2019). The media group's office is located in a prestigious St Petersburg location: in the Lakhta Plaza complex, just next to the Gazprom skyscraper. Concord Management and Consulting, owned by Prigozhin, developed the complex. In October 2019, four St Petersburg media outlets merged under the aegis of Patriot: Federal'noye agentstvo novostey, Ekonomika segodnia, Politika segodnia, and Narodnye Novosti. The online editions of Patriot reached 68.3 million unique visitors per month, according to a statement on the media group's website in (Patriot Media Group, 2023). In 2022-23, Patriot sported a yellow and black ribbon indicating its support for the 'special military operation' on its homepage. Its stated goal was to create 'a favorable information space aimed at the development of the country' and counter 'media, including anti-Russian media, which promote negative information and overlook the good that is happening in the country'. Its website stated: 'Russia is a great and indivisible power, and we must keep it that way for future generations. Patriotism is love for one's country, respect for its culture and traditions' (Patriot Media Group, 2023).[4]

While Prigozhin's info ops abroad – especially in relation to their influencing of the US elections in favour of Donald Trump – are quite well known (Mayne, 2022; Pavlova, 2022), his role in eliminating domestic criticism is not as known, but not less important. Domestically, the media entities that were owned by Prigozhin have specialised in mimicking investigative journalism methods to try to discredit intrepid journalists daring to criticise the regime. These attacks were often carried out by FAN (Federal News Agency) outlets, a part of the Patriot Group. This role of a 'political killer' became very important as Putin was trying to get rid of the oligarchs' hold on the media. Three info ops stand out. There were repeated attacks on Dmitry Muratov, the founder and editor of Novaya Gazeta – four of whose journalists, including Anna Politkovskaya, were killed. In 2019, an opposition member of the St Petersburg Legislative Assembly, Maxim Reznik, was detained during the May Day demonstration; about an hour after his arrest, the FAN ran a story titled 'MP Reznik high as a kite ruined the May 1 holiday for St Petersburg residents'. There was no evidence in the material that the deputy used drugs, other than a reference to an unnamed source. This was followed by other libellous and

[4] However, soon after Prigozhin's aborted rebellion against Russia's military establishment in late June 2023, Patriot announced it was shutting down its operations in Russia (Hancock, 2023). At the time of writing (summer 2023), it remained to be seen whether this cessation of activities was to be temporary or permanent.

unfounded allegations (New Vision, 2019). Lyubov Sobol, a lawyer and opposition activist close to Alexey Navalny, has also been repeatedly attacked in the FNA investigations. One of them was a story alleging that Sobol had staged an attack on her husband in order to get a promotion at Navalny's Anti-Corruption Foundation (FAN, 2019). Sobol claims that Prigozhin's people assaulted her husband to stop Navalny's investigation against him.

Western professional services have often assisted unsavoury individuals from autocratic regimes and Prigozhin is no exception. In January 2023 it was revealed that not only had Prigozhin made use of the services of UK lawyers to attack an investigative journalist (Bellingcat's Eliot Higgins) who published revelations on his activities, but that a unit of the UK Treasury had granted licences for a British law firm to work on his case, approving key steps along the way, which allowed Prigozhin to circumvent sanctions (Fitzpatrick, 2023). The risks of the phenomenon of 'transnational kleptocracy' are clearly illustrated by this case.

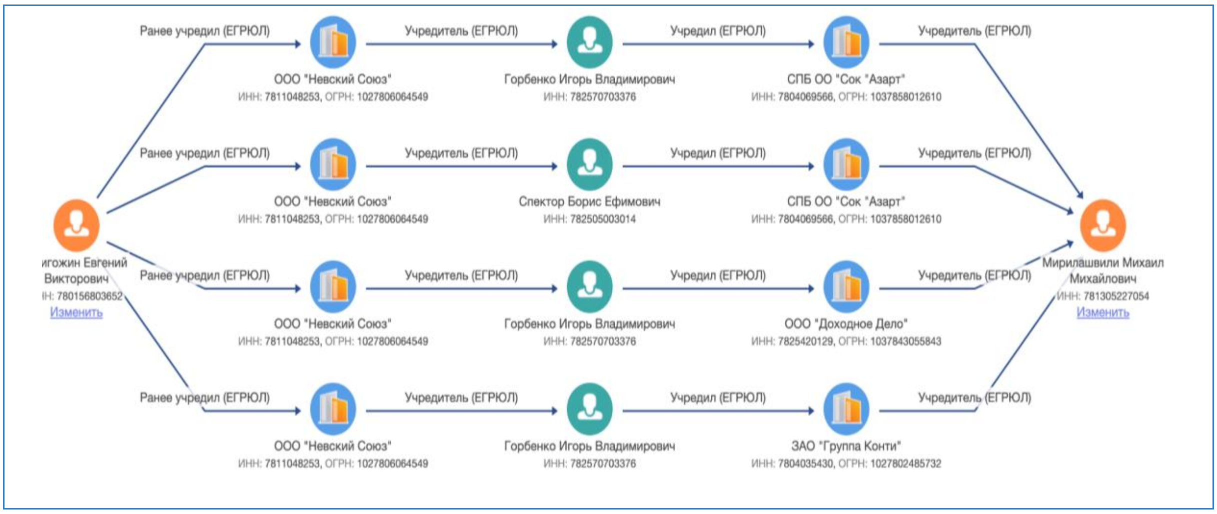
4.2.1. Continued OC ties and Prigozhin's 'coming out'

Initially, Prigozhin denied links with the Internet Research Agency, as well as the insistent allegations that his bot farm and other media spin efforts were involved in the influencing of the 2016 US elections. But, as with other spheres of Russia's activities abroad, the veil has fallen after the all-out invasion of Ukraine. Prigozhin, too, came out of the shadows and became much more outspoken. In February 2023, he confirmed to a group of reporters from the German magazine Der Spiegel that he was the founder of the Internet Research Agency, saying:

> 'I was never just a financier of the Internet Research Agency. I invented it, I created it, I ran it for a long time. It was created to protect the Russian information space from the boorish aggressive propaganda of anti-Russian theses by the West.' (Buschek et al., 2023)

Prigozhin's ties with organised crime go back to his first arrest for robbery in 1979, when he was sentenced to a two-year prison term. He was arrested again in 1981, this time not only for robbery but also for larceny and for engaging juveniles in criminal activity. After being released as a result of the amnesties given in the 1990s, he got immediately involved in the St Petersburg restaurant business. His partners at the time included billionaire Mikhail Miralishvili – also known as 'Misha Kutaissky', a mobster who used to own a TV channel in the 1990s – and Boris Spektor (founder of the Conti Casino) (Meduza, 2021). His dealings earned him the title of 'Person of the Year in Organized Crime and Corruption' for 2022 – a 'prize' given every year by the journalist network Organized Crime and Corruption Reporting Project. As evidenced by the Russian central business registry (egrul.nalog.ru), business ties between Prigozhin and Miralishvili remained active in January 2023 (see Figure 5 below).

Figure 5: Business ties between Evgeny Prigozhin and OC figure Mihail 'Kutaissky' Miralishvili, 2023



Source: Business registry of the Russian Federation (egrul.nalog.ru), January 2023.

Ostensibly, Prigozhin's emboldening became his own downfall. During the full-scale invasion of Ukraine, he openly lamented Russia's military actions and lack of support for his Wagner Group mercenaries. In March 2023, leaked documents from Prigozhin's IT department showed that his companies were testing new hires with a polygraph for FSB ties (Dossier Center, 2023), while in summer 2023 he went as far as launching the fast-aborted mutiny. This is indicative of the competition among branches of the government and security services in Russia, as well as of the shifting sands in the Russian power structures post-February 2022. Prigozhin might have hoped that, through his Kremlin-connected activity, he had become so powerful as to challenge the Kremlin itself. However, the power wielded by him in various spheres – of which the ability to mobilise people through his information appeal was key – had become a two-edged sword for the Kremlin, too sharp to be ignored.

4.3. Transnistria's mobster empire

This case study explores how two mobsters who won the wars in Transnistria, Viktor Gushan and Ilya Kazmaly, built a corporation that now owns over half of the unrecognised republic, and established a media channel that helped them promote politicians willing to write off hundreds of millions of dollars owed by their business empire, in tax and toll exemptions. Gushan and Kazmaly used their political influence and media to remove an oppositional president and send him and his team to prison for 5-16 years.

The Sheriff Holding company, owned by Gushan and Kazmaly, dominates Transnistria's economy, accounting for 60% of it. The corporation includes the primary TV channel, publishing house, and mobile phone network (Argumentum, 2016). Both owners fought in the Soviet police during the Transnistrian war. Gushan was a senior criminal police operative in the early 1990s, working with a mobster named Stanislav Alekseenko, also known as Stas. In 1993, Gushan left the police force after public accusations of his connections to organised crime. In the same year, he and Stas founded Sheriff LLC, which later got in conflict with Nikolay Drozhinkin, also known as Kievskii, who tried to kill Gushan. Stas was killed, and Gushan and his former boss from his time in the criminal police, Ilya Kazmaly, fled to Russia. They returned in 1994, backed by Russian mobsters, and over the next four years, eliminated all competitors, gaining control of all racket schemes in Transnistria. According to journalist investigations, Gushan removed all potential competitors (Sergeevich, 2016). In 1997, Gushan and Kazmaly started a campaign for Transtelecom, the most significant media holding in Transnistria. They created Interdnestrcom, which controls all telecommunications in Transnistria, has the fourth largest coverage in Ukraine, and has a presence in Moldova and annexed Crimea (Kuznetsova, 2017).

Gushan, the owner of Sheriff Holding, is one of the wealthiest people in the post-Soviet area, with a fortune estimated at $2.1 billion (Argumentum, 2016). In 2014 alone, his declared income was 350.8 million transnistrian rubles ($34 million), and in 2013 it was 486.3 million transnistrian rubles ($44 million). Gushan controls the net profit of Sheriff itself, and other companies that are part of the holding.

Sheriff's primary media asset is the TV channel 'Телевидение свободного выбора' (TSV), which has an audience of 400,000 people and broadcasts throughout Transnistria. Cable services and radio stations are secondary to the political influence of TBC (Kuznetsova, 2017). TSV was established in November 1999 by Sheriff, initially broadcasting programmes from the Russian STS entertainment channel, music shows, and sports. TBC began producing news and political shows in 2000, joining the construction of a political agenda. An investigation by Nezavisimaya Gazeta revealed that TBC has an opaque financial scheme and backs the Republican Party 'Renovation', whose representatives control the channel (Tarasov, 2015).

Initially, Sheriff LLC was the sole owner of TSV. In 2009, TSV was replaced by a non-profit organisation named 'TV and Radio Company "Objective"'. However, this was also owned by Sheriff LLC, and Gushan and Kazmaly were the owners (Tarasov, 2015). The partners used a non-profit organisation to avoid taxes and structured the channel's funding as Sheriff's donations to an NGO.

The traditional goal of post-Soviet oligarch-owned mass media is to manipulate the political agenda and arrange appointments of politicians affiliated with business to get bonuses from the authorities. In Sheriff LLC's case, politicians write off the company's debts and provide tax exemptions. According to a Moldovan investigation, between 2013 and 2016 the authorities wrote off over $250 million of debt owed by Sheriff LLC (RISE Moldova, 2016). This happened when the parliament was already governed by Gushan's Renovation party.

Sheriff's political campaigns went smoothly until 2010, when one of the first leaders of Gushan's Renovation party, Evgeny Shevchuk, started his own political career: he was elected president in 2011, and started his own party named Revival. Shevchuk attempted to put checks on Sheriff by exerting political control. However, in 2015, Gushan's Renovation party, with TSV backing, won a majority in parliament. Shevchuk attempted to push through a law on the nationalisation of the largest media companies, but he was outplayed by the leader of the Renovation party, Vadim Krasnosel'sky, who became the president in 2016. Gushan's revenge was severe: in 2018, Shevchuk was charged with bribery and sentenced to 16 years, while his deputies and ministers were imprisoned for between three and 16 years (Elihina, 2020).

4.3.1. Narratives pushed by Sheriff

All Transnistrian media sources align with the agenda of Russia and frequently translate its content. However, TBC has a distinctive approach as it criticises the West, with a focus on Moldova as a NATO puppet promoting warmongering (see, for example, TSV (2023a)). This narrative gained momentum following the enactment of the 2023 anti-separatist law in Moldova. TBC advocates for rejecting existing forms of negotiations with Moldova, echoing Gushan's major interest in remaining the de facto ruler of Transnistria. The channel frequently highlights the significance of Sheriff and Gushan for Transnistria (TSV, 2023b, March).

4.4. The Kremlin's capture of the media

4.4.1. Oligarchisation: Russian media ownership in the 1990s

During the period from 1991 to 1999, Russia witnessed a flourishing era of mass media, particularly television, driven by the infusion of free capital and the absence of state censorship or pressure. This unprecedented growth of television's influence was largely attributed to the investments made by Russian oligarchs in the country's independent media. These oligarchs, tightly linked to OC groups, acquired television channels and newspapers, engaging in fierce internal competition and manipulation of political agendas. Their ownership of media outlets not only bolstered their existing influence on public opinion but also exerted considerable sway over the new Russian government (Reporters Without Borders, 2019). In 1990s Russia, oligarchs' fortunes were made almost overnight in processes of OC-linked privatisation of state-owned enterprises that came to be known as 'grabitisation' (Wedel, 2003, p. 142). Such 'institutional nomads' engaged in large-scale looting, asset-stripping and capital flight (Wedel, 2003, p. 142). These elite actors' ties with organised crime, then endemic in Russia's big business, are therefore well known (Frisby, 1998; Berezovsky v Abramovich, 2012).

One prominent oligarch in this media landscape was Boris Berezovsky, the wealthiest and most influential figure of his time. In the early 1990s, Berezovsky and his business partner Badri Patarkatsishvili – a Georgian-born oligarch who ended up acquiring a variety of media outlets himself – were involved in the so-called Great Mob Wars, allegedly using the Chechen mafia as a 'krysha' (protection) against the Solntsevo crime syndicate (Lemieszewski, 2005; Klebnikov, 2000). Patarkatsishvili served as the primary intermediary between Berezovsky and both the Chechen mafia and the Georgian mafia.[5] After a hot period characterised by shootouts, a realignment with new alliances in the OC space brought a period of stability that allowed oligarchs to infiltrate government structures more easily (Varese, 2001). The contacts between oligarchs and OC, however, did not subside. In 1995, a gangster admitted to the Moscow police that

[5] Badri held the official position of 'deputy chairman of the board of directors of LogoVaz'. In Georgia, one of Badri's brothers, Mareb Patarkatsishvili, held the title of 'vor v zakone', a mafia boss, while his other brother, Levan, held the rank of 'avtoritet', an under-boss position ranking just below a 'vor' in the Georgian mafia.

they had been contacted by Patarkatsishvili about a contract murder; the target, media mogul and advertising competitor Vlad Listyev was indeed killed on 1 March 1995, though the case was never solved (Lemieszewski, 2005; Klebnikov, 2000).

Berezovsky held ownership in various important companies, including the LogoVaz conglomerate, the United Bank, and the Siberian Oil Company (together with Roman Abramovich). In 1994, the creation of Public Russian Television (ORT), the largest channel in the Soviet Union, saw Berezovsky's involvement as a shareholder. The presidential decree allotted 36% of ORT's shares to the state itself, 9% to RGTRK Ostankino, and 8% to banks Menatep (Mikhail Khodorkovsky), United Bank, and Berezovsky's LogoVaz LLC. The first board of directors of the ORT included Anatoly Chubais, Vitaly Ignatenko, Alexander Yakovlev, and Boris Berezovsky (Stream Park, 2021). Additionally, Berezovsky became a stakeholder in the Moscow Independent Broadcasting Corporation (TV-6) and took over the Kommersant Publishing House, which encompassed multiple TV channels, radio stations, newspapers, and magazines (The Times, 2013; RIA Novosti, 2013).

Vladimir Gusinsky, another significant media tycoon, founded the newspaper Segodnya and established the television company NTV in 1993. He further expanded his media holdings in 1997 through the ZAO Media-Most conglomerate, which included NTV, NTV+, TNT television companies, the Segodnya newspaper, and various magazines and radio stations. In 2000, Gusinsky also ventured into online media with the co-ownership of New Media Internet and the publishing house Ostrov (RIA Novosti, 2011).

Berezovsky and Gusinsky emerged as key players in the media landscape, with their respective media outlets shaping public discourse and exerting influence over political developments. Berezovsky was considered the real master of the Kremlin, a grey cardinal in the shadow of Boris Yeltsin. He invested in the first state television channel, turning it into a modern media outlet. His main competitor, Gusinsky, created Russia's first independent television channel, NTV, which quickly developed a sharp and critical style and attacked Yeltsin. NTV faced accusations of providing informational support to the Chechen separatist movement, and its journalists frequently exposed alleged corruption involving prominent politicians.

The private media outlets represented a counterforce to the state-controlled media and became synonymous with freedom and reliable information. They played a crucial role in uncovering the truth about the first Chechen war (1994-96), influencing public opinion and prolonging Russia's involvement in the conflict. However, during the second Chechen war (1999-2000), media coverage was notably scarce (Reporters Without Borders, 2019).

Certain programmes on the Berezovsky-connected ORT channel, such as Sergei Dorenko's 'Author's Program', regularly revealed compromising information about notable Russian politicians. Dorenko accused figures like Anatoly Chubais and Alfred Koch of corruption and aired a press conference featuring Alexander Litvinenko, who openly criticised Vladimir Putin. Eventually, Berezovsky and Putin reached an agreement to halt the information campaign against the future president. Dorenko shifted his focus to denouncing Putin's political rivals, notably Mayor Yuri Luzhkov and Prime Minister Yevgeny Primakov, with accusations ranging from involvement in murder to personal scandals. Gusinsky's NTV, on the other hand, was believed to have supported the Primakov-Luzhkov political bloc during the 1999-2000 election race, although former NTV general director Yevgeny Kiselyov denied this (NewsRu, 2011).

Overall, this period witnessed the rise of oligarch-controlled media as a powerful tool for shaping public opinion, influencing political dynamics, and exposing corruption. The media landscape became a battleground for competing interests and an important factor in Russia's socio-political landscape.

4.4.2. De-oligarchisation: Russian media ownership from the 2000s

In 1998, the Russian government began to express concerns about the state of the media landscape. During the same year, the establishment of the All-Russian State Television and Radio Broadcasting Company (VGTRK) commenced. These initiatives were spearheaded by Minister of Press Mikhail Lesin, who would later play a role in the creation of the television channel Russia Today. Notable players in the media sphere included the National Media Group (REN-TV, Channel 5, Izvestia, STS) and Gazprom-Media Holding, headed by individuals like Minister of Press Mikhail Lesin and representatives of Gazprom. With parliamentary and presidential elections on the horizon, Boris Berezovsky placed his support behind Putin, while Gusinsky openly opposed him. Following Putin's victory in the 2000 presidential election, the dynamics of the television market underwent a significant transformation.

Vladimir Gusinsky's Media-Most and his NTV television company became the primary targets. A protracted struggle unfolded from the spring of 1999 to the spring of 2001. Gusinsky faced charges of large-scale fraud, with scrutiny of his loans from Gazprom, a semi-state company, raising questions from the Kremlin, FSB, and Prosecutor's Office. The government justified the criminal case against Gusinsky on economic grounds, while the media tycoon and his supporters believed it to be politically motivated. Alfred Koch, who sided with Gazprom in the economic conflict, later acknowledged the political nature of the case (Kachkaeva, 2010). The confrontation with NTV culminated in the forcible seizure of the eighth floor of the Ostankino television centre in April 2001, during which Gusinsky was briefly imprisoned in Butyrsky prison. Minister of Press Mikhail Lesin personally signed ‘Protocol No. 6’, which ensured freedom for NTV's principal shareholder, Vladimir Gusinsky, in exchange for control over the television company (Kara-Murza, 2013).

Although Berezovsky thought that he had gained favour with the new president, Putin eventually curtailed the influence of both Gusinsky and Berezovksy, utilising a rhetoric of consolidation in the face of Chechen rebellion, the war on terror, and other mobilising narratives. In April 2001, Boris Berezovsky offered former NTV journalists employment at the TV-6 channel under his control. However, TV-6 was taken off the air in January 2002, citing a law that was no longer in effect at the time (Kara-Murza, 2013).

Following the Kursk submarine disaster and the subsequent (critical) ORT report on the event, Berezovsky met with Alexander Voloshin, the head of the presidential administration, who relayed Putin's message. Putin urged Berezovsky to relinquish his stake in ORT to the state to avoid a situation similar to what happened with Vladimir Gusinsky. Subsequently, Putin met with Berezovsky’s partner Badri Patarkatsishvili – himself a key figure at ORT – and proposed that he and Berezovsky get out of ORT.

Negotiations for the sale of the channel were authorised with Minister of Press and Mass Communications Mikhail Lesin, and the channel's price was set at $300 million. In February 2001, Boris Berezovsky sold his shares in ORT to the state (Gerashenko, 2011).

In the ensuing years, control over major media outlets shifted to the state and individuals or companies loyal to Putin. This included the National Media Group (led by AO Bank Rossiya, with main shareholder Yuri Kovalchuk being a friend of Putin), VGTRK (controlled by the Russian government), Gazprom-Media (owned by PJSC Gazprom, headed by Alexei Miller), Mail.ru Group, and the Kommersant Publishing House (owned by Alisher Usmanov) (BBC, 2014).

4.5. Albania: OC-state equilibrium

Albania's democracy has been fluctuating since the collapse of communism thirty years ago, with some progress but also setbacks. Despite the downfall of one of Eastern Europe's most authoritarian communist regimes in 1990, Albania's democracy has not fully consolidated and is still considered a 'transitional or hybrid regime' according to Freedom House (2023). The country's recent political history can be divided into two phases: the first dominated by the Democratic Party under Sali Berisha from 1992 to 2013, and the second led by the Socialist Party under Edi Rama from 2013 to the present. Although there was optimism about Rama's administration and its potential for reform, progress in the fight against corruption has been slow, and analyses from local and international watchdogs indicate that the trend has been rather towards increasing state capture (Vurmo et al., 2021). In the last two years, however, the efforts aimed at reforming the judiciary have started to bear some fruit, with the jailing of three former ministers and a number of high-level officials for corruption (Freedom House, 2023).

The media landscape reflects this meandering trajectory, with a deteriorating situation in recent years. Following decades of government control over the press, the 1990s and 2000s saw the emergence of independent media, but they faced mounting political pressure and varying journalistic standards due to a lack of adequate regulation. While some legislative changes were carried out, the situation did not improve substantially, with worrying signs of late that legal activism by the government may be used to cement control over the media. Most international watchdogs record a worsening situation in terms of media freedom, highlighting increased attempts by the government as well as the opposition to control the media space; the capture of the media by political and economic elites and power brokers who use it for their own narrow interests; smear campaigns and attacks on journalists; legal and rhetorical attacks by politicians; and – unsurprisingly – rampant self-censorship (ECPMF, 2023).

Media ownership is heavily concentrated in the hands of a select group of "businessmen"-turned-media magnates (or, in some cases, journalists-turned-businessmen) who use media to further their interests. About eight families, all tied to politics, control most of the media scene and 'use these platforms to lobby their interests and maintain close ties with political parties' (Freedom House, 2022). Politics, business and the media are thus closely connected. The organised crime element is very prominent in this nexus. Many outlets are used to spread news with a certain spin, to conduct smear campaigns, or for extortion against politicians and other influential people.

The trends of 'tabloidisation' alongside a proliferation of online content, the declining professional standards and the virtual absence of fact-checking are clear drivers of fake news. This occurs in a context in which journalists are forced to churn out large quantities of clickbait, all the while fighting for their own survival due to very low and precarious wages; and where media owners are using their outlets to further their business or political interests and smear adversaries. Citizens are increasingly distrustful of journalists and journalism and do not know which news can be believed and which cannot. The public's media literacy is very low – which makes the potential for disinformation high. The extreme proliferation of TV talk shows, with pundits spreading unverified information and often espousing a certain 'spin', compounds this problem.

The largest commercial channels are Top Channel and Klan TV, whose popularity and reach today far exceeds that of the public broadcaster: they are both the most profitable channels and those that receive most state funding; their combined reach sometimes exceeds 70% of the audience share (Erebara, 2023a). They were awarded the first two national licences given to commercial TV companies in 2001. Top Channel grew rapidly in the early 2000s: under the leadership of founder Dritan Hoxha, the channel brought in talented staff, and in 2003 it was able to cover all of Albania's territory with its signal, while in 2004 it started transmitting in Europe through the pay-per-view platform DigitAlb, also founded by Hoxha. Hoxha is said to have earned his initial capital through drug smuggling in the early 1990s; in 1993, he established Lori Caffe, which seems to have helped him launder money. Hoxha founded Top Channel in 2001. He was, at the time, the sole shareholder of the company Top Channel LLC. He died in 2008 crashing his Ferrari into a tree near Tirana, and his media empire was thence managed by his widow Vjollca and her four children. In 2022, the Hoxha family sold a large amount of shares, but the new share owners are not known; these changes at Top Channel have been accompanied by episodes of violence (Agence France-Press, 2023).

Klan TV has a national license, while also transmitting through the satellite and digital terrestrial platforms of DigitAlb. It features both entertainment and information, and it has also opened a news channel called Klan Plus, which enjoys a large audience share. Klan TV is owned by the Frangaj family – former journalist Aleksandar Frangaj and his wife Alba Gina. While they are seen as being close to the current government, they have successfully managed to switch sides over the past two decades. Frangaj was accused of being the main beneficiary of a series of government-sponsored advertisement campaigns between 2008 and 2010 (while the Democratic Party was in power) and this trend of profiting handsomely from the state's advertising budget continued with the administration that followed. Gina was previously co-owner of the sports digital platform Supersport, which was sold and merged with DigitAlb in 2016.

Vizion Plus features a mix of entertainment, sport and informative programmes. It is owned by the company Media Vizion, which has been wholly owned by the three Dulaku brothers (Adrian, Artan and Genci) since 2012, through their construction company Edil al Group. Each of them has 33% of shares in the company. The Dulaku brothers and their wives (Ridvana, Holta and Melina) control a string of companies, which are identified as part of Edil al Group and Tring TV. They are seen as having close ties with Edi Rama and with the current mayor of Tirana, Erion Veliaj.[6] In 2016, they were accused of censoring one of their investigative shows that was due to broadcast a critical story on the treatment of waste in Tirana. They – as well as other TV owners – enjoy lucrative building contracts issued by the municipality of Tirana.

Among the television channels operating without a national license, a few more deserve mention. Syri TV stands out as an influential outlet closely aligned with the Democratic Party, although its true ownership remains uncertain. While journalist Çim Peka serves as the public face of the TV station, there are rumours suggesting that the son of Sali Berisha, who is widely accused of collaborating with OC and subject to sanctions by both the USA and the UK, might be the ultimate owner. Syri TV's strenuous defence of the project constructing the biggest skyscraper in Tirana, which is linked to Berisha Jr, is a case in point (Tema, 2023). Two more outlets, Ora News TV and Channel One, have frequently criticised the government. However, in the summer of 2020, a special appeal court accused them of involvement in organised crime. Consequently, the administration of the two channels was taken over by officials from the interior ministry, who alleged that the owner, Ylli Ndroqi, was suspected of drug trafficking. This move drew condemnation from Reporters Without Borders.

Criticism is met with repression, which is most often obfuscated and only rarely brought to the surface (ECPMF, 2023). A stark example is that of News 24 Albania, an outlet that was initially favourably inclined towards the Rama administration. Once it started reporting critically about the government, the outlet was fined by tax inspectors (Erebara, 2023b) and a hotel in Durres belonging to one of its owners was demolished over claims of illegal construction (Erebara, 2022).

The case study of Albania therefore presents a different dynamic when compared with the situations in Transnistria, Russia, and Ukraine. Rather than a competition or unsettlement between OC and the state, Albania exhibits a precarious equilibrium between the two, with a close nexus between politics, business, and the media. Media ownership is concentrated in the hands of a few businessmen-turned-media magnates who use media outlets to further their own interests and engage in smear campaigns. The largest commercial channels are owned by families with connections to political elites. The situation is further complicated by allegations of collaboration with OC and government attempts to control the media space, leading to concerns about media freedom and authoritarian tendencies.

4.6. Takeaways

The analysis of each case study reveals distinct patterns in the relationship between OC and the state, as well as the intensity of information manipulation (IM) activity. Each table, outlining this relationship for each case study, has two axes: Y (the column) represents the degree of integration of OC with the state, whereas X (the row) indicates

[6] Veliaj, in particular, enjoys very positive coverage in Albania virtually across the board; however, messages have emerged exposing his threats to a journalist who has dared criticise him (Politiko, 2023).

the intensity of the information manipulation activity. Development through time is represented by the numbers of the entries, where present.

Case 1. Russian cybercrime

OC-IM nexus: Russian cybercrime				
Integration		1.Pawns (pre-war)		2.Pawns (as war progresses)
Alliance			2.Decoys (as war progresses)	
Enforcement-evasion	1.Decoys (pre-war)			
Confrontation				
Integration (column)/ Intensity (row)	**Low**	**Moderate**	**High**	**Very high**

Russian cybercrime groups are here classified into two categories based on their interaction with the Russian state. **Pawns** are state-sponsored or state-linked cyber groups, such as the hackers linked to the GRU that were analysed in this case study. **Decoys** are the independent, or less dependent, cybercrime groups such as the ransomware syndicates analysed here. It has been shown that, in both cases, the intensity of their IM activity has increased in preparation for, and even more after the start of, Russia's invasion of Ukraine. In addition, the level of integration of the Decoys with the Russian state has increased from more sporadic activity (Enforcement-evasion) – that was aimed at ensuring that the state does not meddle in their affairs – to a higher level (Alliance), where the group decided to (or was forced to?) declare allegiance to the Russian cause in the conflict.

Case 2. Prigozhin, the social media and violence adhocrat

OC-IM nexus: Prigozhin (adhocrat)				
Integration			1.Earlier stage (ad hoc use of bots and Wagner Group for Kremlin aims)	
Alliance				
Enforcement-evasion				2. Intermediate stage (all-in servicing of Kremlin aims while ostensible opposition emerges)
Confrontation				3. Final stage (open confrontation and final showdown)
Integration (column)/ Intensity (row)	**Low**	**Moderate**	**High**	**Very high**

Although initially refusing to acknowledge that his activities were aimed at fostering the foreign policy aims of the Kremlin, it is now abundantly manifest that OC-linked oligarch Prigozhin was doing just that for a long time. In recent years, he was open about being behind both the infamous troll farm and the even more infamous Wagner Group, which the Kremlin later no longer made a mystery of funding. He even bragged about his role in manipulating the US elections in 2016 (whether it had an effect or not, the admission was clear). His pro-Kremlin influencing activity, while high before the invasion of Ukraine, increased exponentially after the full-scale invasion, through his role as the head of the Wagner Group.

With the war in Ukraine unfolding, Prigozhin's activity in service to the Kremlin became as high as ever or perhaps higher, but his level of integration with the Russian state structures experienced profound cracks. The public disputes with Shoigu and the Ministry of Defence, with video messages distributed frequently on social media channels, raised questions about whether the intra-elite conflict was staged or genuine. These were put to rest with the subsequent mutiny attempt by Prigozhin in June 2023 and the downfall of Prigozhin in the August 2023 plane crash. This shows the mercurial nature of the use of adhocrats in large-scale operations of information manipulation, and could offer a cautionary tale for other authoritarian regimes on how this relationship can backfire, while indicating a weakness in the system. Through his control over media, social media, and the means of violence (especially in a region as key as Africa) Prigozhin amassed considerable power, making him difficult – though, as it turned out, not impossible – to dispose of.

Case 3. Transnistria mobster empire

OC-IM nexus: Transnistria (OC captures media, then politics)				
Integration				2. Later stage (consolidating power)
Alliance				
Enforcement-evasion				
Confrontation				1.Earlier stage (unleashing media machine against opponent)
Integration (column)/ Intensity (row)	**Low**	**Moderate**	**High**	**Very high**

The Transnistrian case study illustrates a more straightforward scenario: a situation of confrontation between political opponents where OC-linked individuals captured the media and used information manipulation to beat their opponent (the former president) and solidify their power.

Case 4. Russian media ownership from the 1990s to the Putin era

OC-IM nexus: Russian media ownership (politics captures media from oligarchs)				
Integration				2. Later stage (Kremlin takes control over media, tightening the grip)
Alliance				
Enforcement-evasion		1. Early stage (oligarchs make moderate use of their media machine for political ends)		
Confrontation				
Integration (column)/ Intensity (row)	**Low**	**Moderate**	**High**	**Very high**

The development of Russian media ownership has gone in the opposite direction: it has seen politicians (the Kremlin) make a decisive move against the oligarchs (many of which were linked to OC, and who co-existed until then at a level of either Enforcement-evasion or Alliance with the Kremlin) and take the media over from them. While the media were hardly free from information manipulation earlier, after Putin's takeover the situation became even more bleak, with complete control over the information sphere.

Case 5. Albanian media ownership

OC-IM nexus: Russian media ownership (politics captures media from oligarchs)				
Integration			The relationship remains by and large stable, without confrontation	
Alliance				
Enforcement-evasion				
Confrontation				
Integration (column)/ Intensity (row)	**Low**	**Moderate**	**High**	**Very high**

Contrasting with this, the Albanian case demonstrates a mutually beneficial equilibrium between the ruling elite and OC even before the rise of the Socialist Party, but also a solidifying of these relationships when it did come to power. Both sides coexist, with OC-linked media owners and ruling party officials exchanging government-related advertising and favours. Episodes of confrontation are only occasional and play out in cases where the government uses financial and administrative levers to 'rein back' outlets whose messaging has strayed. While there are pockets of limited media independence and a comfortable hold on power by the ruling party (which is the reason why IM is not classified as 'very high'), the level of IM remains 'high'. It remains to be seen if these equilibria will be disrupted if the ruling party's grip on power weakens, which is not a prospect at the time of writing. Past experience suggests that media owners will align with the prevailing power.

5. Conclusion and next steps

This research paper delved into the intricate relationship between information manipulation and OC, shedding light on a previously unexplored nexus. It proposed a new framework to better understand the dynamics and implications of this complex interplay – unpacking the levels of integration between OC and state structures, as well as the varying intensity of the manipulation employed. The case studies examined in this paper have illustrated the diverse manifestations of this phenomenon across different contexts. The hope is for this conceptual framework to provide a solid foundation for understanding the integration of OC with information manipulation activities. With it as a starting point, other researchers and analysts may find it useful to further test and develop the framework by investigating different empirical material and contexts.

Three connected avenues for further research emerge as valuable to highlight. First, and in addition to probing the information manipulation-OC nexus, future research might also explore the receptiveness of publics to disinformation. While this dimension was not the focus of this evidence review, understanding the factors that contribute to individuals' vulnerability and susceptibility to manipulated information is crucial for developing a comprehensive understanding of the broader information ecosystem. This emerged clearly, for instance, in the examples of Albanian and Russian media ownership control, but it no doubt affects each and every case of information manipulation.

Second, the paper has highlighted the mercurial nature of the ties between elite actors, and especially those between oligarchs or 'adhocrats' and authoritarian regimes – as exemplified by the Transnistrian case and, even more plainly, by Evgeny Prigozhin. His increasing involvement in activities in service to the Kremlin, particularly during the war in Ukraine, boosted his profile and influence. However, this coincided with a noticeable weakening of his integration with Russian state structures, culminating in the mutiny attempt and the eventual demise of Prigozhin in the August 2023 plane crash. This complex interplay between elite actors and the state underscores the risk that building ties that are too strong can backfire, revealing a weakness in the system. It highlights the vulnerability of such relationships and serves as a cautionary tale for other authoritarian regimes, while offering possible lessons for the policy response in fighting authoritarianism.

Third, and related, the insights presented here underscore the pertinence of applying the 'strength of weak ties' framework (Granovetter, 1973) to the examination of elite actors operating in the domain of information manipulation and organised crime. As evidenced by the case of Russian cybercrime, the utilisation of cybercrime groups within an uncodified sphere has afforded the Russian state the ability to maintain plausible deniability concerning its true objectives for an extended period. This dynamic becomes even more pronounced within the realm of information manipulation, where the deliberate cultivation of uncertainty provides a broader operational landscape. In the context of propaganda, it becomes evident that merely sowing the seeds of doubt can be more effective than attempting to persuade individuals to believe otherwise.

A hypothesis emerging from this analysis posits that authoritarian states wield greater latitude in the realm of information manipulation when their connections to the OC-affiliated groups executing such campaigns on their behalf exhibit intermediate – rather than high – levels of integration. This divergence in network strength appears to grant these actors a significant advantage, allowing them to operate with increased opacity and, consequently, greater influence over the dissemination of manipulated information. Probing the nature of the ties between OC and the state constitutes, therefore, another promising avenue for further research.

Annex: Criminal groups

1. GRU-linked hackers (Russia)

- Country: Russia
- Brief bio: GRU-linked hackers are state-sponsored or state-linked cybercrime groups associated with the Russian military intelligence agency, GRU. They engage in various illicit activities, including cyberattacks, data theft, and disruption of critical systems.

2. Ransomware syndicates (global)

- Country: Global
- Brief bio: Ransomware syndicates are independent or less dependent cybercrime groups operating worldwide. They specialise in deploying ransomware attacks to encrypt victims' data and demand ransom payments in exchange for decryption keys.

3. Troll farm (Russia)

- Country: Russia
- Brief bio: The troll farm refers to an infamous group that was involved in information manipulation and online propaganda. It is known for orchestrating social media campaigns aimed at shaping public opinion and promoting specific agendas.

4. Wagner Group (Russia)

- Country: Russia
- Brief bio: The Wagner Group is an OC-linked private military contractor believed to have close ties to the Russian government. It has been involved in various conflicts and operations, providing military support and conducting activities aligned with Russian foreign policy interests.

5. Transnistrian Mobster Empire (Transnistria)

- Country: Transnistria
- Brief bio: The Transnistrian Mobster Empire refers to a criminal network operating in the region of Transnistria. This group has captured media outlets and utilised information manipulation to consolidate its power and influence in the region.

Note: The information provided in this annex offers a brief overview of the criminal groups mentioned and their general activities. For more detailed information, further research and exploration of additional sources are recommended.

References

Abbate, L., & Gomez, P. (2007). I Complici: Tutti gli uomini di Bernardo Provenzano da Corleone al Parlamento. Fazi Editore.

Adebanwi, W., & Obadare, E. (2011). When corruption fights back: democracy and elite interest in Nigeria's anti-corruption war. The Journal of Modern African Studies, 49(2), 185-213. https://doi.org/10.1017/S0022278X11000012

Agence France-Presse. (2023, March 27). Guard killed in gun attack on Albanian TV channel. https://www.voanews.com/a/guard-killed-in-gun-attack-on-albanian-tv-channel-/7023379.html

Alyukov, M. (2022). Making sense of the news in an authoritarian regime: Russian television viewers' reception of the Russia–Ukraine conflict. Europe Asia Studies, 74(3), 337-359. https://doi.org/10.1080/09668136.2021.2016633

Argumentum. (2016, July 2). Олигархи Приднестровья «прячут» бизнес в Украине (Oligarchs of Transnistria "hide" business in Ukraine). АРГУМЕНТ. https://argumentua.com/stati/oligarkhi-pridnestrovya-pryachut-biznes-v-ukraine

Auerbach, J., & Castronovo, R. (2013). Introduction: Thirteen propositions about propaganda. In R. Castronovo & J. Auerbach (Eds.), The Oxford Handbook of Propaganda Studies (pp. 1-16). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199764419.013.023

Barnes, N. (2017). Criminal politics: An integrated approach to the study of organized crime, politics, and violence. Perspectives on politics, 15(4), 967-987. ProQuest. 10.1017/S1537592717002110

Bartlett, J. (2016). The dark net: Inside the digital underworld. Melville House.

BBC. (2014, July 11). Who owns the media in Russia: leading holdings (Кто владеет СМИ в России: ведущие холдинги). BBC Russian Service. https://www.bbc.com/russian/russia/2014/07/140711_russia_media_holdings

BBC. (2019, December 4). 'This is not Prigozhin': how 'Patriot' fights 'anti-Russian media' ('Это не Пригожин': как 'Патриот' борется с 'антироссийскими СМИ'). https://www.bbc.com/russian/features-50632900

Berezovsky v. Abramovich. (2012). Royal Courts of Justice. EWHC 2463 (Comm). 31 August 2012. https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/berezovsky-judgment.pdf

Buschek, C., Christoph, M., Diehl, J., Höfner, R., Hoffman, H., Hoppenstadt, M., Lehberger, R., Müller, A., Obermaier, F., Obermayer, B., Rosenbachg, M., Schultz, T., & Wiedman-Schmidt, W. (2023, February 20). How a covert firm spreads lies and chaos around the world. Der Spiegel. https://www.spiegel.de/international/world/inside-the-covert-firm-that-spreads-lies-and-chaos-around-the-world-a-3c55e1cd-7d61-4cf8-8321-999da1996aa8

Camut, N. (2023, June 27). Putin admits Kremlin gave Wagner nearly $1 billion in the past year. Politico. https://www.politico.eu/article/vladimir-putin-yevgeny-prigozhin-russia-kremlin-gave-wagner-group-nearly-1-billion-in-the-past-year/

Chen, J. & Xu, Y. (2017). Information manipulation and reform in authoritarian regimes. Political Science Research and Methods, 5(1), 163-178. https://doi.org/10.1017/psrm.2015.21

Deutsche Welle. (2022, January 15). US 'welcomes' Russian arrests of REvil ransomware gang. https://www.dw.com/en/us-welcomes-russian-arrests-of-revil-ransomware-gang/a-60432637

Dossier Center. (2023, March 18). Кибервойска Пригожина (Prigozhin's cyber troops: How the IT infrastructure of Wagner, Troll Factory and Concorde works). Dossier Center. https://dossier-center.appspot.com/prig-it/

Dutka, D. (2006). Violent non-state actors in world politics: their formation, actions, and effects. PhD thesis, Pennsylvania State University.

ECPMF. (2023, July 19). Defending media freedom and journalists' safety in Albania. https://www.ecpmf.eu/defending-media-freedom-and-journalists-safety-in-albania/

Edmond, C. (2013). Information manipulation, coordination, and regime change. The Review of Economic Studies, 80(4), 1422–1458. https://doi.org/10.1093/restud/rdt020

Elihina, Y. (2020, November 18). Shevchuk and his team. What happened to the people of the ex-head of Transnistria. (Шевчук и его команда. Что стало с людьми экс-главы Приднестровья). NewsMaker. https://newsmaker.md/rus/novosti/shevchuk-iego-komanda-chto-stalo-slyudmi-eks-glavy-pridnestrovya/

Erebara, G. (2022, September 2). Albania Mogul Says Govt Targeting His Media Over Editorial Line. Balkan Insight. https://balkaninsight.com/2022/09/02/albania-media-mogul-claim-government-attacked-his-businesses-over-editorial-line/

Erebara, G. (2023a, August 11). Klan and Top Channel dominate the television market in the country. (TVSH, Klan dhe Top Channel dominojnë tregun televiziv në vend). Reporter.al. https://www.reporter.al/2023/08/11/tvsh-klan-dhe-top-channel-dominojne-tregun-televiziv-ne-vend/

Erebara, G. (2023b, February 28). Albanian Tax Inspectors Fine Critical Media Outlets. Balkan Insight. https://balkaninsight.com/2023/02/28/tax-inspectors-issue-heavy-fines-for-several-media-outlets/

Espiner, T., & Tidy, J. (2023, January 12). Royal Mail hit by Russia-linked ransomware attack. BBC. https://www.bbc.com/news/business-64244121

FAN. (2019, June 10). Media: FBK lawyer Lyubov Sobol staged an attack on her husband to get promoted. (СМИ: Юрист «ФБК» Любовь Соболь инсценировала нападение на мужа ради повышения в должности). RIA. https://newdaynews.ru/moskow/664263.html

Fitzpatrick, J. (2023, January 23). How Rishi Sunak's Treasury helped Putin ally sue Bellingcat's Eliot Higgins. openDemocracy. https://www.opendemocracy.net/en/prigozhin-government-russia-ukraine-hack-libel-slapp/

Freedom House. (2022). Albania. Nations in Transit 2022 report. https://freedomhouse.org/country/albania/nations-transit/2022

Freedom House. (2023). Albania. Nations in Transit 2023 report. https://freedomhouse.org/country/albania/nations-transit/2023

Frisby, T. (1998). The rise of organised crime in Russia: Its roots and social significance. Europe-Asia Studies, 50(1), 17-49.

Galeotti, M. (2020, August 22). Russia's murderous adhocracy. The Moscow Times. https://www.themoscowtimes.com/2020/08/22/russias-murderous-adhocracy-a71219

Gardner, A. (2011). Democratic governance and non-state actors. Palgrave Macmillan.

Garmazhapova, A. (2013, September 7). Where trolls live, and who feeds them. (Где живут тролли. И кто их кормит). Novaya gazeta. https://novayagazeta.ru/articles/2013/09/07/56253-gde-zhivut-trolli-i-kto-ih-kormit

Gerashenko, E. (2011, July 11). According to documents, Boris Berezovsky received $10 million for 49% of ORT. (По документам за 49% ОРТ Борис Березовский получил $10 млн), Kompromat.ru. https://www.compromat.ru/page_31432.htm

Granovetter, M. S. (1973). The strength of weak ties. American Journal of Sociology, 78(6), 1360-1380. https://www.jstor.org/stable/2776392

Hancock, E. (2023, July 2). Wagner Group boss shutters media empire. Politico. https://www.politico.eu/article/wagner-group-boss-yevgeny-prigozhin-shutter-patriot-media-empire/

Heathershaw, J., Sharman, J., & Cooley, A. (2018). The rise of kleptocracy: Laundering cash, whitewashing reputations. Journal of Democracy, 29(1), 39-53.

Heathershaw, J., Cooley, A., Mayne, T., Michel, C., Prelec, T., Sharman, J., & Soares de Oliveira, R. (2021, December 8). The UK's kleptocracy problem: How servicing post-Soviet elites weakens the rule of law. Chatham House. https://www.chathamhouse.org/2021/12/uks-kleptocracy-problem

Heathershaw, J., Prelec, T. & Mayne, T. (forthcoming in 2024). Professional indulgences: British service providers, postcommunist elites, and the enabling of kleptocracy. Oxford University Press.

Hughes, H. C., & Weismel-Manor, I. (2021). The Macedonian fake news industry and the 2016 US Election. PS: Political Science & Politics, 54(1), 19-23. https://doi.org/10.1017/S1049096520000992

Hutchinson, S. & O'Malley, P. (2007). A crime-terror nexus? Thinking on some of the links between terrorism and criminality. Studies in Conflict Terrorism, 30(12), 1095-1107.

Insikt Group. (2021, September 9). Dark covenant: Connections between the Russian state and criminal actors. Recorded Future. https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf

Insikt Group. (2023, January 31). Dark covenant 2.0: Cybercrime, the Russian state, and the war in Ukraine. Recorded Future. https://go.recordedfuture.com/hubfs/reports/cta-2023-0131.pdf

Josselin, D., & Wallace, W. (Eds.) (2001). Non-state actors in world politics. Palgrave.

Jung, H. M. (2009). Information manipulation through the media. Journal of Media Economics, 22(4), 188-210. https://doi.org/10.1080/08997760903375886

Kachkaeva, A. G. (2010). The history of television in Russia: between power, freedom and property (История телевидения в России: между властью, свободой и собственностью). Istoriya Novoy Rossii. http://ru-90.ru/node/1316

Kara-Murza, V. (2013). The Kremlin speaks and shows. 10 years without independent television («Говорит и показывает Кремль». 10 лет без независимого телевидения). Institut Sovremennoy Rossii. https://www.imrussia.org/ru/politics/1496-the-kremlins-voice-10-years-without-independent-tv-in-russia

Klebnikov, P. (2000). Godfather of the Kremlin: The decline of Russia in the age of gangster capitalism. Harcourt Inc.

Kumar, M., & Fowler, S. (2023, January 18). Scrutiny of LockBit3.0 ransomware gang intensifies. Oxford Analytica. https://dailybrief.oxan.com/Analysis/ES275389/Scrutiny-of-LockBit30-ransomware-gang-intensifies

Kuznetsova, A. (2017). Contemporary mass media system in Transnistria: perspectives for development (СОВРЕМЕННАЯ СИСТЕМА СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ПРИДНЕСТРОВЬЯ: ПЕРСПЕКТИВЫ РАЗВИТИЯ). Philological Sciences. Questions of theory and practice. (Филологические науки. Вопросы теории и практики), 6(1), 24-28. https://www.gramota.net/materials/2/2017/6-1/6.html

Lemieszewski, S. (2005). Boris Berezovsky and Badri Patarkatsishvili. SOC culture Russian – Narkive. https://soc.culture.russian.narkive.com/fE6hW8hK/boris-berezovsky-and-badri-patarkatsishvili

Makarenko, T. (2004). The crime-terror continuum: Tracing the interplay between transnational organised crime and terrorism. Global Crime, 6(1), 129-145.

Makarenko, T. & Mesquita, M. (2014). Categorising the crime-terror nexus in the European Union. Global Crime, 15(3-4), 259-274.

Maksimović, S. & Burazer, N. (2021, March 9). Serbian government weaponized state-owned Telekom to curb media freedom? European Western Balkans. https://europeanwesternbalkans.com/2021/03/09/serbian-government-weaponized-state-owned-telekom-to-curb-media-freedom/

Mayne, T. (2022, May). Russian illicit financial flows and influence on western European politics. SOC ACE Research Briefing Note No. 9. University of Birmingham. https://www.birmingham.ac.uk/documents/college-social-sciences/government-society/publications/russian-illicit-financial-flows-briefing.pdf

McCornack, S. A. (1992). Information manipulation theory. Communication Monographs, 59(1), 1-16. https://doi.org/10.1080/03637759209376245

Meduza. (2021, June 15). За что в 1981 году в СССР судили Евгения Пригожина, которого теперь весь мир знает как «повара Путина». Публикуем текст судебного документа. (For which in 1981 Yevgeny Prigozhin was tried in the USSR, whom the whole world now knows as "Putin's cook." We publish the text of the court document.). Meduza. https://meduza.io/feature/2021/06/15/za-chto-v-1981-godu-v-sssr-sudili-evgeniya-prigozhina-kotorogo-teper-ves-mir-znaet-kak-povara-putina-publikuem-tekst-sudebnogo-dokumenta

Microsoft Digital Security Unit. (2022, April 27). An overview of Russia’s cyberattack activity in Ukraine [Special report: Ukraine]. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Mpoke Bigg, M. (2023, August 24, updated August 30). What to know about the plane crash that killed Yevgeny Prigozhin. The New York Times. https://www.nytimes.com/2023/08/24/world/europe/prigozhin-plane-crash-russia-wagner.html

Nershi, K., & Grossman, S. (2022, October 7). Assessing the political motivations behind ransomware attacks [Working paper]. Stanford Internet Observatory. https://bahamasamlconference.centralbankbahamas.com/assets/images/pdf/conferences/2023/nershi-grossman_ransomware.pdf

NewsRu. (2011, April 15). NTV, 10 years after the change of ownership, still stirs interest: Kiselev responds to Yumasheva’s accusations. (НТВ спустя 10 лет после смены владельца будоражит умы: Киселев ответил Юмашевой на обвинения). https://www.newsru.com/russia/15apr2011/vokrugntv.html

New Vision. (2019, May 5). Максим Резник переждет нарко-скандал в Чехии. Новый Взгляд (Maxim Reznik will wait out the drug scandal in the Czech Republic). https://newvz.ru/info/149997.html

OECD. (2022, November 3). Disinformation and Russia’s war of aggression against Ukraine: Threats and governance responses. Organisation for Economic Co-operation and Development (OECD). https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/

OpenMedia. (2019, October 4). «Повар Путина» Пригожин возглавил совет медиагруппы «Патриот». В нее вошли медиа, связь с которыми он всегда отрицал. Открытые Медиа сообщают). (“Putin's Chef” Prigozhin headed the board of the Patriot media group. It included the media, the connection with which he always denied. https://openmedia.io/news/povar-putina-prigozhin-vozglavil-sovet-mediagruppy-patriot-v-nee-voshli-media-svyaz-s-kotorymi-on-vsegda-otrical/

OSCE. (2012, March 5). Observers detail flaws in Russian election [Press release]. https://www.oscepa.org/en/news-a-media/press-releases/press-2012/observers-detail-flaws-in-russian-election

Owen, C., Prelec, T., & Mayne, T. (2022, May 5). The illicit financialisation of Russian foreign policy: Mapping the practices that facilitate Russia’s illicit financial flows. SOC-ACE Research Paper No. 3.

University of Birmingham. https://www.birmingham.ac.uk/documents/college-social-sciences/government-society/publications/illicit-financialisation-of-russian-foreign-policy-report.pdf

Pacepa, I. M., & Rychlak, R. J. (2013). Disinformation: Former spy chief reveals secret strategies for undermining freedom, attacking religion, and promoting terrorism. WND Books.

Paraschiv, G. (2013). Conceptualising transnational organized crime. Economics, Management and Financial Markets, 8(2), 173-178.

Parfitt, T. (2012, February 4). Anti-Putin protesters march through Moscow. The Guardian. https://www.theguardian.com/world/2012/feb/04/anti-putin-protests-moscow-russia

Patriot Media Group. (2023). О медиагруппе. Медиагруппа «Патриот». Retrieved June 27, 2023, from https://mediapatriot.ru/about [Now taken down; for the original text, see: https://web.archive.org/web/20230627122619/https://mediapatriot.ru/about]

Pavlova, U. (2022, November 7). Russian oligarch Prigozhin appears to admit to US election interference. CNN. https://edition.cnn.com/2022/11/07/europe/yevgeny-prigozhin-russia-us-election-meddling-intl/index.html

Perri, F. S. & Brody, R. G. (2011). The dark triad: organized crime, terror and fraud. Journal of Money Laundering Control, 14(1), 44-59.

Persson, A., Rothstein, B., & Teorell, J. (2010). The failure of anti-corruption policies: a theoretical mischaracterization of the problem [Working Paper]. Gothenburg University Library. https://gupea.ub.gu.se/handle/2077/39039

Politiko. (2023, July), Erion Veliaj's threatening messages to the journalist are published. https://politiko.al/english/e-tjera/foto-publikohen-mesazhet-kercenuese-te-erion-veliajt-ndaj-gazetares-i487713

Pomerantsev, P. (2014). Nothing is true and everything is possible: The surreal heart of the New Russia. Public Affairs.

Popov, V. (2005). The relationship between the mass media and organised crime in post-Soviet Russia: a sociological perspective. [Unpublished doctoral thesis]. City University, London. https://openaccess.city.ac.uk/id/eprint/8475/1/The_relationship_between_the_mass_media_and_organised_crime_in_post-Soviet_Russia-_a_sociological_perspective.pdf

Prelec, T. (2020, December 7). Regime change and the rule of law: Serbia's lessons to Montenegro. European Western Balkans. https://europeanwesternbalkans.com/2020/12/07/regime-change-and-the-rule-of-law-serbias-lessons-to-montenegro/

Reporters Without Borders (2019, April 24). The oligarchs go shopping (Олигархи идут за покупками). https://rsf.org/sites/default/files/oligarques3-ru_0.pdf

RIA Novosti (2013). Boris Berezovsky, one of the most odious oligarchs of the 'dashing 90s' in Russia, has died. (Скончался Борис Березовский - один из самых одиозных олигархов "лихих 90-х" в России). https://ria.ru/20130324/928713266.html

RIA Novosti (2011, July 27). 'Vladimir Alexandrovich Gusinsky' (Владимир Александрович Гусинский). https://ria.ru/20110727/408088899.html

RISE Moldova. (2016, May 3). The Sheriffs of the Transnistrian Media (Шерифы приднестровских СМИ). Rise Moldova.

Rocha Menocal, A. (2022, June). Incorporating organised crime into analysis of elite bargains and political settlements: Why it matters to understanding prospects for more peaceful, open and inclusive politics. SOC-ACE Programme, Briefing note No. 21. University of Birmingham.

Sanderson, T. M. (2004, January). Transnational terror and organized crime: Blurring the lines. SAIS Review, 24(1), 49-61.

Schenkkan, N., Linzer, I., Furstenberg, S., & Heathershaw, J. (Eds.). (2020, July). Perspectives on "everyday" transnational repression in an age of globalization. Freedom House. https://freedomhouse.org/sites/default/files/2020-07/07092020_Transnational_Repression_Globalization_Collection_of_Essays_FINAL_.pdf

Sergeevich, S. (2016, November 17). Sheriff. Transnistria. Business in the 1990s. Illusion of deception part 1 (Шериф. Приднестровье. Бизнес 90-е. Иллюзия обмана часть 1). YouTube. https://www.youtube.com/watch?v=9kUbr8xoKyE

Shelley, L. I. (2018). Dark commerce: How a new illicit economy is threatening our future. Princeton University Press. https://doi.org/10.2307/j.ctv346n56

Šmid, T. (2014, September 1). The organized crime-terrorism nexus in post-Soviet Chechnya, Mezinarodni Vztahy (Czech Journal of International Relations), 49(3), 26-42.

Stonor Saunders, F. (1995, October 22). Modern art was CIA 'weapon'. The Independent. https://www.independent.co.uk/news/world/modern-art-was-cia-weapon-1578808.html

Stream Park (2021, February 10). 'First channel'. History of the country's main TV channel («первый канал». История главного телеканала страны). https://stream-park.ru/blog/pervyj-kanal-istoriya-glavnogo-telekanala-strany/

Tema. (2023, 8 August), The tower in Tirana that disturbed the Berisha family (Kulla e Tiranës që trazoi familjen Berisha). https://www.gazetatema.net/politika/kulla-e-tiranes-qe-trazoi-familjen-berisha-i401724

Tarasov, S. (2015, November 13). Formation of oligarchic media in Transnistria (Становление олигархических СМИ в Приднестровье / СНГ). Nezavisimaya Gazeta. https://www.ng.ru/cis/2015-11-13/100_smi131115.html

The Times (2013, March 25). Boris Berezovsky: Russian businessman whose influence grew after the break-up of the Soviet Union but who fled from President Putin to come to the UK. https://www.thetimes.co.uk/article/boris-berezovsky-85g6lt77ndd

TSV. (2023a, February 4). Sit down, separatist, you'll get two [years in prison]. (Садись, сепаратист, тебе два) [Video]. YouTube. https://www.youtube.com/watch?v=D9PHvm903Ac

TSV. (2023b, March). Swimming for the little ones at the Sheriff Sports Complex'(Плавание для самых маленьких на СК «Шериф») [Video]. YouTube. https://www.youtube.com/watch?v=XtFHe9KVCGk&feature=youtu.be

Varese, F. (2001). The Russian mafia: Private protection in a new market economy. Oxford University Press.

Vurmo, G., Sulstarova, R., & Dafa, A. (2021). Deconstructing state capture in Albania: An examination of grand corruption cases and tailor-made laws from 2008 to 2020. Transparency International / Institute for Democracy and Mediation (IDM).

Wedel, J. (2003). Dirty togetherness: Institutional nomads, networks, and the state-private interface in Central and Eastern Europe and the former Soviet Union. Polish Sociological Review, 142, 139-159.