Oude Waalsdorperweg 63
2597 AK Den Haag
Postbus 96864
2509 JG Den Haag

www.tno.nl

T +31 88 866 10 00
F +31 70 328 09 61

**TNO 2020 S11273**

# Fighting from the Shadows

## The Role of Criminal Actors in Hybrid Warfare

| | |
|---|---|
| Datum | 24 August 2020 |
| Auteur(s) | Niels van Gent (s2411113)<br>*Master Crisis and Security Management* |
| Copy no | 1 |
| No. of copies | 1 |
| Number of pages | 62 (incl. appendices) |
| Number of appendices | 1 |
| Sponsor | TNO |
| Supervisors | Peter van Scheepstal; Giliam de Valk (Leiden University) |
| Second reader | Jelle van Buuren (Leiden University) |
| Project name | V1925 Hybride Dreigingen |
| Project number | 060.38374 |

# Summary

Understanding war is a quest scholars have embarked upon almost as long as the concept exists. Many have tried to grasp the nature of war or, more realistically, try to understand the mode of war in their time. One of the newest concepts that does this, is hybrid warfare. Modern warfare is less about large armies fighting each other, and more about states using all possible means and methods to reach their goals. This thesis focuses on the case of Russia in the context of hybrid warfare. Since its subversive operations since the Cold War, the country is still active on many different fronts, from cyberattacks to military intervention in the conflict in East-Ukraine. The Kremlin has a wide range of actors at its disposal; both state and non-state actors. This thesis studies the role of criminal actors in Russian hybrid warfare, with a focus on the threat this poses to the Netherlands. Using a literature study and scenario building, the use of criminal actors in Russian hybrid operations is not seen as a direct threat, but a potential threat. With this analysis, several lessons are identified for policy makers to monitor the development of this threat and improve the resilience of the Netherlands against it.

# Contents

# 1 Introduction

As one of the key elements of human existence, war has always been a subject of study. The motivation for studying war vary greatly: some study it to improve one's tactics and beat the opponent, others to better understand politics. The continually changing face of warfare makes it an all the more interesting subject of study. Weapons and tactics change at a high rate, due to technological developments and shifting alliances. However, our traditional understanding of war as a conflict between two or more armies of a country seems barely applicable to today's wars.

## 1.1 Context

In the last decade, the term *hybrid warfare* is often used to describe the modern-day conflict. This form of warfare characterised by 'blurring': it creates a situation where it is unclear whether a state of war exists – and if it does, who is a combatant and who is not.[1] As in traditional warfare, states are the main players, given that only states have the resources and organising capabilities to wage hybrid warfare. One of the states often mentioned in the context of hybrid warfare, is Russia. Especially since the annexation of Crimea in 2014, literature on the topic of 'Russian hybrid warfare' surged.[2] Hybrid warfare is seen as a key element of Russia's geopolitical behaviour, dating back to Soviet Union strategy and tactics referred to as *subversion* or *active measures.*[3] In the study of this topic, a large part of the literature is focused on the definition and conceptualisation of (Russian) hybrid warfare. Although this is a useful debate, this thesis will focus on a different aspect: the actors involved. A wide range of actors can be used, from state actors such as the army and the intelligence services, to non-state actors like companies or mercenaries. Although these actors are studied extensively in academia, there is little research on the role actors play in hybrid warfare. [4]

Criminal actors are often mentioned in relation to the concept of hybrid warfare, but rarely studied in detail. This thesis will do so, and thereby improve the understanding of the role criminal actors play in hybrid warfare, specifically in the Russian context. First, an analysis of hybrid warfare and the Russian approach to it is done, followed by an analysis of Russian criminal actors.
Building on this understanding, scenarios and critical indicators are developed that focus on the threat these actors could pose to the Netherlands in the future.

[1] Rod Thornton, "The Changing Nature of Modern Warfare: Responding to Russian Information Warfare," *The RUSI Journal* 160, no. 4 (2015): 40–48, https://doi.org/10.1080/03071847.2015.1079047.
[2] Bettina Renz, "Russia and 'Hybrid Warfare,'" *Contemporary Politics* 22, no. 3 (2016): 283–300, https://doi.org/10.1080/13569775.2016.1201316.
[3] Andrew Radin, Alyssa Demus, and Krystyna Marcinek, *Understanding Russian Subversion: Patterns, Threats, and Responses* (RAND Corporation, 2020), https://www.rand.org/pubs/perspectives/PE331.html.
[4] Magnus Normark, "How States Use Non-State Actors : A Modus Operandi for Covert State Subversion and Malign Networks," 2019, 1–8.

## 1.2 Relevance

Despite the amount of research on this topic, further research is necessary. The term *hybrid* has gained popularity in policy and academia, but is at the same time heavily debated: the range of different interpretations and conceptions of *hybrid* has made it difficult to distinguish a clear concept of analysis. It is therefore important to look beyond the academic debate and the use of the term in policy, and study the reality of what *hybrid warfare* tries to describe. Doing so has value for both academia and society.

*Academic relevance*
The academic debate on hybrid warfare and its variations focuses mainly on the entire battlespace. However, there is little research on the types, roles and relationship of actors within this battlespace.[5] Studying the role of criminal actors in hybrid warfare in a specific country would improve this understanding and build a model of analysis that could be applied to other countries or types of actors.

*Societal relevance*
Studying criminal actors in Russian hybrid warfare gives an in-depth understanding of an actor type and its role in the hybrid domain. This understanding can help policymakers in deciding whether or not a country should develop a response to this threat, and if so, what response would be the most efficient for this specific threat. More specifically, this study is done at TNO, in the context of the research program 'Hybrid Threats', commissioned by the Dutch Ministry of Defense.

## 1.3 Research question

This topic will be studied using the following research question:
*How can Russia use criminal actors in the concept of hybrid warfare in the Netherlands?*

To come to a conclusive answer to this question, the following sub-questions will be answered:

1 How did the concept of hybrid warfare develop?
2 What is the concept of hybrid warfare?
3 What is the Russian approach to hybrid warfare?
4 How can the role of actors in Russian hybrid warfare be analysed?
5 What is the role of criminal actors in Russian hybrid warfare?
6 How can the role of criminal actors be detected?
7 How can this role be expected to develop in the future, specifically in the Netherlands?

## 1.4 Readers guide

This thesis is divided into 8 chapters, of which this introduction is the first. In chapter 2, the methodology of this thesis will be outlined, followed by a thorough background of hybrid warfare that is developed in chapter 3 and 4. These chapters give a clear view on the concept of hybrid warfare, its origins and the Russian approach to it. Furthermore, the role of actors in Russian hybrid warfare is discussed, and a

[5] Frank G Hoffman, "Conflict in the 21st Century:," n.d., 72.

conceptual framework of actor analysis is developed. Chapter 5 will focus on criminal actors and their origins, structure, presence in the Netherlands and finally their activities in the context of hybrid warfare. In chapter 6, a driver analysis is done using a SWOT analysis and a Causal Loop Diagram, which generates the drivers for this threat. From the two highest-ranking drivers, four scenarios are developed in chapter 7, and the implications of these scenarios outlined. Finally, the conclusion and answer to the research question is given in chapter 8, which ties together the different elements of this thesis.

# 2 Methodology

Before going into the analysis section, it is important to define the methodological approach of this thesis. This study will not conduct traditional academic research, but intelligence research, which has a significantly different methodological approach. There are three types of intelligence research: descriptive, explanatory and prognostic research.[6] This study will combine all three types, starting with a descriptive approach of Russian criminal actors. Next, the link between criminal actors and Russian hybrid warfare will be made, which is explanatory research. Finally, scenarios and indicators are developed to monitor future developments, which is prognostic research. In this chapter, the methodological choices for this thesis are explained.

## 2.1 Alpha & beta

An important distinction in the methodological approach of intelligence research is the different aim. In traditional academic research, the goal is to formulate or test theories. The focus is therefore on the *alpha*: "the chance that you *incorrectly* conclude that there is a significant relationship between phenomena", i.e. a false positive.[7] The aim of academic research is to have a low alpha. Intelligence analysis on the other hand, focuses on the *beta*: the chance that you do *not* discover a weak, but an existing relationship between phenomena, i.e. a false negative.[8] It is important to have a low beta, as it is essential to not miss existing relationships in a case, albeit weak ones. These two concepts are also known as Type I and Type II errors in statistics; the Type I error relating to the alpha, the Type II error to the beta. In intelligence research, detecting possible threats is more important than proving the correctness of this threat. This has to do with the possible consequences of missing a (weak) relationship: as intelligence analysis is often on matters of national security, the stakes can be very high. This applies to criminal actors in hybrid warfare as well. Given the shadowy nature of these actors, it is difficult if not impossible to make claims about this threat with full certainty, and the alpha will therefore be high. This is acceptable, as long as the beta is low; not missing possible threats of criminal actors is more important than the measure of certainty of these threats. With the understanding of the possible threat an actor poses, we can better monitor and prepare for this type of threat.

## 2.2 A/B/C-level theory

Most academic research deals with level-A and level-B theory; respectively general theory and practice-oriented theory. The overall aim of intelligence research, however, is not to produce a scientific theory, but is to better monitor future (hostile) actions.[9] It therefore applies level-C theory: studying a single case or context. It is often difficult to come to a clear conclusion based on a single case. The conclusion of this report comes from three layers: (1) it follows from developing the concept of

[6] De Valk, 55.
[7] Giliam G. de Valk, "Dutch Intelligence - towards a Qualitative Framework for Analysis" (University of Groningen, 2005), 41.
[8] De Valk, 41.
[9] De Valk, 52.

criminal actors in hybrid warfare; (2) it follows from the available data on this topic and (3) it follows from logic reasoning, further explained in the paragraph on data analysis. If all three layers are present, it is possible to formulate a strong conclusion which will be the assumption for this moment; until evidence is found that contradicts the conclusion of the report.

### 2.3 Case selection

Academic research on hybrid warfare has amassed over the last few years. A large part of the debate is on the uniqueness of the concept, comparing it to other new or not-so-new versions of warfare. This is an important and relevant debate for a better understanding of modern warfare. However, a good understanding of the actors involved is still lacking. For this reason, the choice was made for a case study, instead of focusing on the concept in general. Secondly, there are several examples of states using criminal actors, ranging from cases of drug trade and terrorist organisations to cyberwarfare. Due to the availability of literature and other non-academic sources, the choice was made for the case of Russian hybrid warfare and criminal actors. There are considerably fewer sources available in other possible cases.

### 2.4 Data collection

This thesis will be written using a variety of openly-accessible sources. These will mostly be secondary sources, such as academic literature and reports by think tanks and research institutions. In addition, primary sources like government reports, hearings and news reports will be used. This data will be collected using both search engines and databases. The part on hybrid warfare will primarily be based on academic literature and policy reports, as these topics are extensively covered in academic and policy circles. For analysing Russian criminal actors, criminology literature will be used, as well as public police reports. Studying criminal networks or state actors using open sources is challenging, as there is little or no evidence of the exact activities of these actors. Conclusions are thus drawn with caution and should not be easily generalized. In addition to these sources, experts on Russian organised crime and hybrid warfare will be consulted in semi-structured interviews, to get a broader view on these matters.

### 2.5 Data analysis

In most academic research, analysis is done using inductive or deductive logic, or a combination of the two. Induction is an inference of a generalized conclusion from particular instances.[10] Deduction is an inference in which the conclusion follows necessarily from general or universal premises, for example applying a theory to a case.[11] A third form is abductive logic, which can be defined as “a syllogism in which the major premise is evident but the minor premise and therefore the conclusion only probable”.[12] There are two interpretations of abduction: the older interpretation sees abduction as a reasoning in *generating* hypothesis, while the modern interpretation

[10] “Induction,” Merriam Webster, 2020, http://www.merriam-webster.com/dictionary/induction.
[11] “Deduction,” Merriam Webster, 2020, http://www.merriam-webster.com/dictionary/deduction.
[12] “Deductive vs. Inductive vs. Abductive Reasoning,” Merriam Webster, 2020, https://www.merriam-webster.com/words-at-play/deduction-vs-induction-vs-abduction.

sees it as *justifying* hypothesis, also called the Inference to the Best Explanation (IBE).[13] This thesis will use all three types of reasoning. First, abductive reasoning conceives different hypotheses or scenarios. Next, deductive reasoning is used to find testable consequences from the scenarios, and induction helps to come to a verdict on the scenarios.[14] This process of analysis is subjective, as the observations are not directly derived from facts; they are interpretations.[15] To deal with this subjectivity, it is important to outline the facts, evidence and analysis leading to the conclusion of the report, which this thesis therefore will do.[16]

[13] Igor Douven, "Abduction ," Stanford Encyclopedia of Philosophy, 2015, https://plato.stanford.edu/entries/abduction/#DedIndAbd.
[14] Igor Douven, "Peirce on Abduction ," Stanford Encyclopedia of Philosophy, 2015, https://plato.stanford.edu/entries/abduction/peirce.html.
[15] Cynthia M Grabo, "Anticipating Surprise: Analysis for Strategic Warning" (Joint Military Intelligence College, 2012).
[16] Paul Wolfowitz, "Intelligence Policy-Relations," *Policy*, 1994, 38.

# 3 Studying Warfare

War has been a defining feature of the world's history: every civilization, every era has experienced war and conflict. How wars are fought, has changed immensely over the years. This dynamic was already recognized by Carl von Clausewitz, a Prussian officer, who noted that every age has its own mode of war, with its own limitations and preconceptions.[17] In the effort to understand the nature of warfare in their particular era, historians, strategists and military leaders have developed a vast array of theoretical perceptions of war and modes of warfare. One of the most recent concepts of warfare and the focus of this thesis is *Hybrid Warfare.* Although this concept has only been used in the last two decades, it is important to analyse the wider theoretical debate that preceded it. This chapter will do so, developing an answer to the first two sub-questions: How did the concept of hybrid warfare develop? and What is the concept of hybrid warfare? Answering these questions gives a better understanding of the concept itself and how it is rooted in the century-old study of war.

## 3.1 Origins

The foundation of the study of war is laid out in three classical works: *On War, The Art of War* and *The Peloponnesian War*, by some called the 'essential trilogy for understanding strategy'.[18] The earliest of these is the book *The Art of War* by Sun Tzu, a Chinese general of the Zhou dynasty in ancient China. A key element of *The Art of War* is that deception is the basis of all warfare: every move you make should be obscured in every way possible.[19] Furthermore, Sun Tzu argues that an army should be highly adaptable, as the battlefield constantly changes: "just as water retains no constant shape, so in warfare there are no constant conditions".[20] Another important early work is the account of the Peloponnesian wars, written by the Athenian *strategos* Thucydides, who started documenting the war as he perceived it as a more important war than any that had preceded it.[21] Next to Sun Tzu and Thucydides, the name of Von Clausewitz is inherently connected to the study of war, as his work has dominated the Western way of thinking about war and peace. Clausewitz compares the theoretical concept of war ('absolute war') with the reality of war, analysing the wars of Alexander the Great to Napoleon. This comparison brings Clausewitz to three lessons. 1: The act of war is never isolated from other domains; 2: the results of war are never final; and 3: chance plays an important role.[22] Building on these three classical works, scholars from all over the world have extended this body of work. Understanding war is an ongoing process and although

[17] Zachery Tyson Brown, "Unmasking War's Changing Character," Modern War Institute, 2019, https://mwi.usma.edu/unmasking-wars-changing-character/.
[18] Colin S. Gray, Fighting Talk : Forty Maxims on War, Peace, and Strategy (Praeger Security International, 2007).
[19] Sun Tzu, The Art of War, ed. Lionel Giles (London: Sterling Publishers Pvt.Ltd, 1994), http://www.gutenberg.org/files/132/132-h/132-h.htm, chapter 1, 18.
[20] Sun Tzu, chapter 6, 32.
[21] Thucydides, "The History of the Peloponnesian War," accessed April 23, 2020, https://history.hanover.edu/courses/excerpts/211thuc.html.
[22] Erik De Landmeter, "The Relevance of Clausewitz's 'On War' to Today's Conflicts," De Militaire Spectator, 2018, https://www.militairespectator.nl/thema/strategie/artikel/relevance-clausewitzs-war-todays-conflicts.

war is universal, its conduct in *warfare* is not: warfare changes constantly and drastically, sometimes in a short period. This drastic change is demonstrated in the conflicts of the last century. Since the two World Wars, the world has seen a shift from inter-state war dominated by conventional means, to conflicts with both state and non-state actors, using military and non-military means and tactics to obtain their goals. This shift is one of the main topics of discussion in the war studies: how to make sense of modern warfare.

### 3.2 Modern warfare

Many different terms have been coined in an effort to describe modern warfare. Although these definitions vary greatly, most do adhere to the division of two main modes of warfare: regular and irregular. In general terms, regular warfare is a conflict between the armed forces of states, and irregular warfare a conflict between a state's armed forces and irregular armed forces of non-state political entities.[23] However, recent conflicts have seen a fusion of both irregular and regular warfare. This development was conceptualised by general James Mattis and Frank G. Hoffman in 2005. The U.S. Marine Corps officers argued that although conventional wars will not disappear and the rise of irregular warfare will continue, the future of warfare will not adhere to these distinctions. Instead, they argued, future warfare will be a "merger of different modes and means", which they called hybrid warfare.[24] Important case studies used to validate his concept are the wars in Afghanistan, Iraq and Lebanon, the first two fought by the US and its allies, the latter by Israel. During these conflicts, armies faced radically different adversaries and tactics. They were not fought between conventional armies, using conventional tactics and means. Instead, concepts like combatants, tactics and the rules of engagement blurred, which required an entirely different way of fighting. Building on the beforementioned concepts of warfare and studies of recent wars, Hoffman defines hybrid warfare as a conduct of war that can be waged by "*both states and a variety of non-state actors. They incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder".*[25] Hoffman's approach is distinctive from other conceptions of warfare, as it develops a more holistic view on warfare by building on both the theoretical study of war, and research on networks, terrorism and urban warfare.[26] Furthermore, it is distinctive in that it addresses the difference in how the adversary plans to fight.[27]

Since its introduction in 2005, hybrid warfare is widely discussed in the academic debate, which has resulted in a wide range of interpretations and uses of the term hybrid. Johnson identifies two general schools of thought on the concept. The first sees hybrid warfare as merely a combination of regular and irregular warfare. The focus in this school is on the military form of war, (along with criminal elements) which calls for a mostly military response.[28] This perception of hybrid warfare has therefore

[23] Colin S. Gray, War, Peace and International Relations: An Introduction to Strategic History, 2nd ed. (New York: Routledge, 2012).
[24] James N Mattis and Frank G Hoffman, "Future Warfare: The Rise of Hybrid Wars," U.S. Naval Institute Proceedings 131, no. 11 (2005): 18–19.
[25] Hoffman, 29.
[26] Hoffman, 30.
[27] Johnson, 147.
[28] Johnson, 146.

limited analytical value, as the focus on the military domain restricts the possibilities of countering hybrid threats, that can affect many different domains. The second school sees hybrid warfare as an inherently new concept, to which new responses have to be developed.[29] The third school in this debate is formed by the critics of the concept. Some state hybrid warfare is not a new concept at all, marking it as 'intellectual laziness' when the concept is used as a label for everything we do not understand.[30] Others state the conceptual confusion is not the issue, but how to clarify the concept in a useful manner is.[31]

### 3.3 Conceptualising warfare

Apart from the debate on hybrid warfare, a wide range of paradigmatic terms to describe phenomena other than conventional war has been developed.[32] Several other concepts 'compete' with hybrid warfare for a general understanding of modern warfare. An early concept in this list is *Fourth-Generation Warfare*. Developed by a group of US officers, the three past generations of warfare are identified and a fourth generation is suggested. Characteristics of this generation are an ideological or religious base, attacks on an enemy's culture and highly sophisticated psychological warfare.[33] In 1998, nine years later, the concept of *Unrestricted Warfare was* developed by two Chinese Colonels. The authors disagree with Von Clausewitz, stating that the "new principle of war is no longer 'using armed force to compel the enemy to submit to one's will', but 'using all means, including armed and non-armed forces, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests.[34] Currently, China's People's Liberation Army (PLA) uses the *Three Warfare* concept*,* which outlines three different strategies: psychological warfare, media warfare and legal warfare.[35] This concept is often used to understand the Chinese way of what the West calls *hybrid warfare.* Another concept that deals with the existence of both regular and irregular forces in wars, is *Compound Wars:* major wars with a significant regular and irregular component, that fight at the same time and under the same command.[36] Compound Wars, Unrestricted Warfare and 4th-generation warfare are the most important theories in Hoffman's concept of hybrid warfare, as he integrates elements of these concepts in his theory.

Other scholars define modern war in general, such as the concept of *New Wars,* developed by Mary Kaldor. Her work characterizes war after the Cold War by four aspects: violence between state and non-state networks, identity politics as a base,

[29] Johnson, 147.
[30] Bastian Giegerich, "Hybrid Warfare and the Changing Character of Conflict," Connections: The Quarterly Journal 15, no. 2 (2016): 76, https://doi.org/10.11610/Connections.15.2.05.
[31] Erik Reichborn-Kjennerud and Patrick Cullen, "What Is Hybrid Warfare?," NUPI Policy Brief 1 (2016), http://brage.bibsys.no/xmlui/bitstream/handle/11250/2380867/3/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf.
[32] Johnson, 145.
[33] William S. Lind et al., "The Changing Face of War: Into the Fourth Generation," Marine Corps Gazette, 1989, https://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html.
[34] Robert J. Bunker, "Unrestricted Warfare: Review Essay I," Small Wars & Insurgencies 11, no. 1 (2000): 114–21, https://doi.org/10.1080/09592310008423265.
[35] Stefan Halper, "China: The Three Warfares," 2013, 1–566.
[36] Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars," 20.

focus on political control of the population rather than physical, and conflict financed through other means than a state.[37] Another popular term is *Grey Zone Warfare,* defined by the U.S. Military as "competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality".[38] In Grey Zone conflicts, the nature of the conflict and the parties involved are unclear, and there is uncertainty about the relevant policy and legal frameworks that apply. A problem with this concept is its wide span: it is used to cover very distinctive conflicts, making it a somewhat unpractical term.[39] *Grey zone warfare* is more and more used in the US debate, whereas the term 'hybrid' is more used in Europe.[40] Lastly, the concept of *Irregular Warfare,* originating from US military doctrine, is used often as well. The US definition is "a violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. IW favours indirect and asymmetric approaches, though it may employ the full range of military and other capabilities in order to erode an adversary's power, influence, and will."[41]

The fight over which concept defines modern war and warfare best, is likely to continue the coming years. However, this thesis will not engage in the conceptual debate but study a specific actor in the geopolitical realm: Russia. This is done through the lens of hybrid warfare for two reasons. First: the concept of hybrid warfare is a useful tool of analysis of the different phases of hybrid warfare, and for the analysis of the opponent.[42] This is particularly relevant for this thesis, as it will study a particular opponent and its use of criminal organisations throughout different phases of hybrid conflict. Second, developing the hybrid warfare concept enables governments to better understand and assess threats towards the state, and develop an appropriate response.[43] To do so, this thesis contributes to a better understanding of the relation between the Russian government and Russian criminal actors. This knowledge is then used to develop scenarios and indicators that can help to assess the threat that is posed by Russian criminal actors in the context of hybrid warfare.

Other terms are used to discuss hybrid warfare, such as hybrid war or hybrid threats. To avoid confusion, it is important to identify these terms. Epistemologically, hybrid warfare is the operational conception, a mode of waging war by combining conventional and unconventional means, tactics and capabilities in a coordinated manner. Hybrid war is a form conflict in which this mode is applied, and a hybrid

[37] Mary Kaldor, New and Old Wars : Organized Violence in a Global Era (Cambridge: Polity Press, 2013).
[38] Philip Kapusta, "The Gray Zone," 2015.
[39] Frank G Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," Prism 7, no. 4 (2012): 31–47.
[40] Vladimir Rauta, "Towards a Typology of Non-State Actors in 'Hybrid Warfare': Proxy, Auxiliary, Surrogate and Affiliated Forces," Cambridge Review of International Affairs, 2019, 1–20, https://doi.org/10.1080/09557571.2019.1656600.
[41] United States of America Department of Defense, "Irregular Warfare (IW) Joint Operating Concept (JOC)," vol. 1, 2007.
[42] Mikael Weissmann, "Hybrid Warfare and Hybrid Threats Today and Tomorrow: Towards an Analytical Framework," Journal on Baltic Security 5, no. 1 (2019): 17–26, https://doi.org/10.2478/jobs-2019-0002.
[43] Kęstutis Kilinskas, "Hybrid Warfare: An Orientating or Misleading Concept in Analysing Russia's Military Actions in Ukraine?," Lithuanian Annual Strategic Review 14, no. 1 (2016): 139–58, https://doi.org/10.1515/lasr-2016-0006.

threat the actor that wages this type of warfare.[44] A hybrid threat is "any adversary that simultaneously employs a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behaviour in the same time and battlespace to obtain their political objectives".[45] In this thesis, the NCTV definition of hybrid warfare is used: "A form of conflict between states, mostly under the juridical level of open armed conflict, with integrated use of means and actors, in order to reach certain strategic goals".[46] The next chapter will zoom in on Russian hybrid warfare, and the Western and Russian perceptions of this concept.

[44] Maria Mälksoo, "Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO," European Security 27, no. 3 (2018): 374–92, https://doi.org/10.1080/09662839.2018.1497984.
[45] Frank G. Hoffman, "On Not-so New Warfare: Political Warfare vs. Hybrid Threats," War on the Rocks, 2014, https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.
[46] NCTV, "Χίμαιρα, Een Duiding van Het Fenomeen 'Hybride Dreiging,'" 2019, 1–36, https://www.nctv.nl/documenten/rapporten/2019/04/18/duiding-fenomeen-hybride-dreiging.

# 4 Russia and Hybrid Warfare

In this chapter, Russian tactics and methods will be analysed, starting with the Cold War-period, followed by the fall of the Soviet Union and the modern day practices of Russian warfare. This part will thereby answer the third sub-question: what is the Russian approach to hybrid warfare? Next, the conceptual framework for the actor analysis is set up, addressing the fourth sub-question: how can the role of actors in Russian hybrid warfare be analysed?

## 4.1 Origins

One event that has had a major impact on the academic debate on hybrid warfare is the annexation of Crimea in 2014. Hybrid warfare was seen as the perfect way to describe the variety of tactics that was used by Russia during this operation, and was quickly adopted by both scholars and analysts, as by policy- and decisionmakers.[47] Although this portrayal is heavily debated,[48] alternative ways of warfare from Russia are anything but new: it has deep historical roots; from the Tsarist Empire to the Soviet Afghan War and the Chechen wars.[49] During the Soviet era, a wide range of methods was used to create a strategic advantage over the adversary; some of which overlap with methods of hybrid warfare. An example of these methods is *subversion,* sometimes called *active measures:* an umbrella term for activities intended to influence a target's country domestic politics, using propaganda, forgery, disinformation or agents of influence.[50] Subversive tactics were extensively used by the Soviet Union in its satellite states, but also in the rest of world.[51] Former KGB officer Oleg Kalugin described subversion as the 'heart and soul of Soviet intelligence',[52] while KGB defector Yuri Bezmenov stated that 85% of KGB actions were focused on subversion, and the remaining 15% intelligence gathering.[53]

The dissolution of the Soviet Union caused a major geopolitical shift and diminished the influence of the new Russian Federation. From a Russian point of view, the

[47] Bettina Renz, "Russia and 'Hybrid Warfare,'" Contemporary Politics 22, no. 3 (2016): 284, https://doi.org/10.1080/13569775.2016.1201316.
[48] Matthew Rojansky and Michael Kofman, "A Closer Look at Russia's 'Hybrid War,'" Kennan Cable, 2015, https://www.wilsoncenter.org/publication/kennan-cable-no7-closer-look-russias-hybrid-war.
[49] Mark Galeotti, "Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?," Small Wars & Insurgencies 27, no. 2 (2016): 282–301, https://doi.org/10.1080/09592318.2015.1129170.
[50] Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," Connections: The Quarterly Journal 15, no. 1 (2016): 7.
[51] Andrew Radin, Alyssa Demus, and Krystyna Marcinek, Understanding Russian Subversion: Patterns, Threats, and Responses (RAND Corporation, 2020), https://www.rand.org/pubs/perspectives/PE331.html.
[52] CNN, "Inside the KGB," 1998, https://web.archive.org/web/20070627183623/http://www3.cnn.com/SPECIALS/cold.war/episodes/21/intervie ws/kalugin/.
[53] Thomas Ricks and Oscar Jonsson, "How Russia Stumbled into a Winning Strategy to Undermine the West," *Foreign Policy*, March 29, 2017, https://foreignpolicy.com/2017/03/29/how-russia-stumbled-into-a-winning-strategy-to-undermine-the-west/.

Colour Revolutions were the result of a Western strategy of regime change.[54] Meanwhile, the power of the West in the form of NATO increased, especially in the former satellite states of the Soviet Union. Despite several promises to Russian officials that NATO would not move eastwards,[55] NATO extended its cooperation with Central European countries and eventually accepted former satellite states as members, starting with Poland, Czech Republic and Hungary in 1999.[56] This process goes directly against an idea deeply embedded in Russian thinking: Russia is a great power and therefore deserves to be treated as such. However, the West does not adhere to this idea: it is constantly trying to 'sweep us into a corner', according to Putin; both during the Cold War and after, making it Russia's biggest threat.[57]

The debate on hybrid warfare related to Russia is a widespread and diffuse one. Not only hybrid warfare is used to describe modern Russian tactics, also concepts like *Political Warfare*, a term coined by U.S. diplomat George F. Kennan, who defined it as "the employment of all the means at a nation's command, short of war, to achieve its national objectives, overt and covert".[58] The issue with this term is, much like the *grey zone* concept, its reach. Political warfare covers a wide array of actions, labelling everything as a form of warfare. However, as it is 'short of war', others argue, it is not a form of warfare.[59]

Ambiguously, Russian military thinkers see hybrid warfare as a Western mode of war that Russia has to protect itself against; an argument put forward by the Russian general Valery Gerasimov. Based on his speech in 2013, Western scholars developed the 'Gerasimov doctrine', misinterpreting Gerasimov's speech as the Russian military doctrine.[60][61] The speech was focused on armed operations in warfare and how subversion can be used as a prelude to war, while Russian strategic thinking has a broader interpretation of warfare than armed operations.[62] One of the Russian strategic concepts is that of *New Generation Warfare*, which uses eight phases, ranging from non-military asymmetric warfare (using information, psychological, economic measures; phase 1) to complete takeover of the opponent (phase 8).[63] This concept of warfare (it is based on the work of two Russian officers)

54 A series of revolutions in Soviet satellite states towards the end of the Cold War, often characterized by a colour like the 'Velvet Revolution' in Czechoslovakia; hence the term 'colour revolutions'.
55 Tom Blanton and Svetlana Savranskaya, "NATO Expansion: What Gorbachev Heard," National Security Archive, 2017, https://nsarchive.gwu.edu/briefing-book/russia-programs/2017-12-12/nato-expansion-what-gorbachev-heard-western-leaders-early.
56 NATO, "A Short History of NATO," NATO Declassified, accessed May 7, 2020, https://www.nato.int/cps/en/natohq/declassified_139339.htm.
57 Thornton, "The Changing Nature of Modern Warfare."
58 Murat Caliskan, Modern Political Warfare: Current Practices and Possible Responses, The RUSI Journal, vol. 164, 2019, https://doi.org/10.1080/03071847.2019.1621490.
59 Hoffman, "On Not-so New Warfare: Political Warfare vs. Hybrid Threats."
60 Valeriy Gerasimov, "Науки В Предвидении," Military Industrial Courier 8, no. 476 (2013): 2–3, https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf.
61 Keir Giles, "Russia's 'New' Tools for Confronting the West," Russia and Eurasia, vol. 1, 2016, https://doi.org/10.1515/sirius-2017-0037.
62 Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine,'" Foreign Policy, 2018, https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.
63 Jānis Bērziņš, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy," no. April (2014): 6.

has been incorporated in the term *New Type Warfare,* the official term now used in Russian military publications to describe modern warfare.[64]

Despite the conceptual debate on Russian doctrine, most Western definitions refer to a core issue: a wide range of Russian activities that aims to influence and undermine countries' politics and institutions in undesirable ways.[65] The Russian strategy behind these activities is not new, as we have seen a similar strategy during the Soviet Era. However, Russia 'updated' or 'tailored' this strategy to the 21st Century, deploying new tactics and making use of a more interconnected, globalised world.[66]

### 4.2 Cases

There are several poignant examples of Russian hybrid activity over the last two decades. The most prominent example is the annexation of Crimea in 2014. Using propaganda, motor gangs and armed forces without insignia, Russian armed forces quickly took over military bases and strategic locations on the Crimean Peninsula. The operation was surrounded by secrecy and confusion: it took a month for the Kremlin to admit that the 'little green men' were indeed Russian forces.[67] Crimea is not the only example of hybrid methods, however. Recent elections in the US and Europe saw serious Russian involvement. During the 2016 US elections, a large disinformation campaign was active; smearing presidential candidate Hillary Clinton, and promoting then-candidate Donald Trump. On a smaller scale, these methods were used in Europe as well, for example in the Brexit campaign and in the French elections. Furthermore, throughout Europe, Russian operatives have been identified for conducting subversive activities, for example the poisoning of Sergei Skripal and his daughter in the United Kingdom.[68] A remarkable feat of these subversive activities is the range of different actors that can be put to use by the Russian government. Radin et al outlined the different organisations that are used for subversion (see figure 1).[69]

[64] Timothy Thomas, "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking," Journal of Slavic Military Studies 29, no. 4 (2016): 554–75, https://doi.org/10.1080/13518046.2016.1232541.
[65] Radin, Demus, and Marcinek, Understanding Russian Subversion.
[66] Christopher Chivvis, "Understanding Russian 'Hybrid Warfare': And What Can Be Done About It" (RAND Corporation, 2017), https://doi.org/10.7249/ct468.1; Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia."
[67] Mark Galeotti, "'Hybrid War' and 'Little Green Men': How It Works, and How It Doesn't," n.d.
[68] BBC News, "Skripal Poisoning: Third Russian Suspect 'Commanded Attack,'" 2019, https://www.bbc.com/news/uk-48801205.
[69] Radin, Demus, and Marcinek, *Understanding Russian Subversion, 9*.

How Do Russian Organizations Engage in Subversion?

| | State | Attributed and Unattributed Proxies | Foreign Partners of Russia | Major Challenges to Target |
|---|---|---|---|---|
| Military | GRU-Spetsnaz; VDV | Private military companies (Wagner Group) | Separatists | • Relatively highly capable light forces<br>• Difficult to distinguish from armed civilians at the beginning; a law enforcement response might be insufficient, while a military response bears political costs and may contribute to Russian propaganda |
| Political | Possibly executed by intelligence agencies (GRU, FSB, SVR) | State-linked patriotic groups (e.g., Night Wolves biker gang) | Ataka in Bulgaria, Front National in France, AfD in Germany | • Political influence in target countries<br>• Attribution to Russian government<br>• Grounded in preexisting political divisions |
| Economic | State-owned enterprises (e.g., Gazprom, Rosneft) | Private, state-linked companies (e.g., Lukoil) | Trade partners with Russia | • Extensive European trade links with Russia<br>• Difficulty distinguishing legitimate activity |
| Information | RT, Rossiya Segodnya, Sputnik, security services | Internet Research Agency (and other troll farms) | Users who amplify Russian media or unknowingly participate—"useful idiots" | • Deceptive or false content<br>• Difficult to regulate<br>• Attribution<br>• Global reach |
| Cyber | GRU, FSB, SVR | Co-opted independent hackers: APT28, APT29 | Patriotic hacking groups: CyberBerkut | • Highly capable<br>• Attribution<br>• Global reach |

SOURCES: Robinson et al., 2018; Helmus et al., 2018; Larrabee et al., 2017; Radin et al., 2019.

Figure 1. Russian Organizations in Subversion (Radin et al, 2020)

With this large palet of actors at its disposal, the Russian government has the ability to target countries worldwide, often under the radar and with relatively little effort. For governments, these threats are challenging to detect or counter: the activities are often obscured and therefore difficult to attribute.

Not only large countries are the target of Russian operations: also smaller countries are targeted. In the Netherlands, Russian influence has been visible for a long time, starting with the Dutch engineer Sebald Rutgers, who in 1918 became a confidant of Lenin and later started the Comintern desk for Western Europe in the Netherlands, funded by the Soviet Union.[70] Around 1950, the Affaire-K came to light: intelligence officers from Czechoslovakia used the embassy in The Hague as their base of operations.[71] Later, an organisation campaigning against nuclear weapons called 'Stop the Neutron bomb', appeared to have been supported with money from the GDR and the Soviet Union, with the involvement of a Dutch member of Parliament, Joop Wolff.[72] More recent examples are Russian efforts to influence the criminal case of MH17 and the attempt to hack the OPCW.[73] Russia's connections to populist political parties is present in the Netherlands as well, as some populist politicians question the reliability of the Joint Investigation Team (the team investigating MH17) and take a pro-Russia standpoint regarding matters such as NATO. This short

[70] Hans Olink, "Sebald Rutgers (1879-1961), Nederlands Ingenieur in de Sovjet-Unie," *Historisch Nieuwsblad*, no. 1 (2014), https://www.historischnieuwsblad.nl/sebald-rutgers-1879-1961-nederlands-ingenieur-in-de-sovjet-unie/.
[71] NISA, "Spionagecentrum in Tsjechoslowaakse Ambassade," Ingelicht § (2002).
[72] de Valk, "Dutch Intelligence - towards a Qualitative Framework for Analysis," 311.
[73] BBC News, "How the Dutch Foiled Russian 'cyber-Attack' on OPCW," 2018, https://www.bbc.com/news/world-europe-45747472; Robert Van der Noordaa and Coen Van der Ven, "Nepnieuws Uit Sint-Petersburg," De Groene Amsterdammer, 2019.

overview of past and recent events demonstrates the Russian interest in the Netherlands as a country, despite its small size.

### 4.3 Actors

The examples of Russian hybrid warfare not only show a variety of methods and tactics, but also a variety of actors. However, we have little knowledge of the "types, roles and relationships involving actors within and across the different domains of action".[74] This thesis deals with this lack of knowledge by studying one actor-type: criminal groups. To get a good understanding of their role in hybrid warfare, the relationship between actors and the possible functions of an actor are analysed, using two models.

The first model deals with relations between actors in hybrid warfare. First, an actor is either a beneficiary, or a proxy. Second, a distinction is made between state actors and non-state actors. With this division, four types of state/non-state relations are possible, which results in the following table:

| | | **Actor b: Proxy** | |
|---|---|---|---|
| | | *State* | *Non-state* |
| **Actor a: Beneficiary** | *State* | I | II |
| | *Non-state* | III | IV |

Figure 2. Beneficiary-proxy relationship (Maurer 2017)

In Russian hybrid warfare, these different types of proxy relationships occur, but not all to the same extent.

*I. State/state proxy relationship*: a state uses another state to do its bidding. It is difficult to prove a type I proxy relationship, as this rarely reaches the public. Distinguishing it from an alliance can be challenging as well: alliances are often equal on paper, but asymmetric in reality.[75]

*II. State/non-state proxy relationship*: states using non-state actors to reach their goals, such as private military contractors. There is a strong focus on this type of proxy relationship in literature on hybrid warfare. Figure 1 (chapter 4.2) gives an overview of the many possible actors with this proxy relationship in the Russian context.

*III. Non-state/state proxy relationship*: in this type, non-state actors benefit from a weak state actor, profiting from or effectively taking over state systems. This can happen on a large scale, such as a political party taking over the power of the state, or on an individual level, where individuals become the state, instead of agents of the state.[76] This non-state/state proxy relationship is present in Russian society, especially since the dissolution of the Soviet Union.

[74] Rauta, "Towards a Typology of Non-State Actors in 'Hybrid Warfare': Proxy, Auxiliary, Surrogate and Affiliated Forces," 2.
[75] Maurer, 33.
[76] Tim Maurer, "Proxies: An Instrument of Power Since Ancient Times," *Cyber Mercenaries* 21 (2017): 33, https://doi.org/10.1017/9781316422724.003.

*IV: Non-state/non-state proxy relationship*: non-state actors, especially powerful ones like large enterprises, make more and more use of other non-state actors.[77] This type of proxy relationships occurs regularly, for example the report from British and American intelligence services that the FSB-linked hacker group Turla used the Iranian-linked hacker group APT34 to gain access to other governments.[78]

The second model classifies actors by their function. Rauta introduces a typology based on non-state actors in military operations, but this typology can be applied to other types of actors as well. The axis of 'relational morphology' refers to the role of the actor; whether a task is delegated, or if the actor supplements a larger force. The axis of 'relational embeddedness' refers to the extent actors are embedded in an operation: directly (operating with the main force) or indirectly (operating alongside the main force).[79] These two models are used as a conceptual framework for studying Russian criminal actors in hybrid warfare.

| | | Relational Morphology | |
|---|---|---|---|
| | | Supplementary | Delegatory |
| Relational Embeddedness | Direct | AUXILIARY | AFFILIATE |
| | Indirect | SURROGATE | PROXY |

Figure 3. Typology of non-state actors (Rauta 2019)

[77] Maurer, 34.
[78] Jack Stubbs and Christopher Bing, "Hacking the Hackers: Russian Group Hijacked Iranian Spying Operation, Officials Say," *Reuters UK*, October 21, 2019, https://uk.reuters.com/article/uk-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUKKBN1X00AX.
[79] Vladimir Rauta, "Towards a Typology of Non-State Actors in 'Hybrid Warfare': Proxy, Auxiliary, Surrogate and Affiliated Forces," Cambridge Review of International Affairs, 2019, 7, https://doi.org/10.1080/09557571.2019.1656600.

# 5 Criminal actors in Russia

After an analysis of the broader context of Russian hybrid warfare, this chapter focuses on the fifth sub-question: what is the role of criminal actors in Russian hybrid warfare? First, the origins of modern criminal groups are analysed, followed by the present situation and new developments. Lastly, the conceptual framework is applied, which gives a comprehensive overview of the role Russian criminal actors play in hybrid warfare.

## 5.1 Origins

The origins of modern-day Russian organised crime can be found in the 19th century. During the Tsarist empire, a criminal subculture called the *vorovskoy mir* ('thieves world') developed; with its own code, language and symbols. The elite of the thieves world was called the *vory v zakone* ('thief-in-law'), a class of 'professional criminals'.[80] During the rule of Stalin, the structure of the thieves world changed significantly. Many criminals were sent to the Gulag, Stalin's labour camps, which enabled the *vory* to build criminal networks.[81] Furthermore, an ideological shift took place: although it was forbidden by the criminal code to cooperate or work for the government, many criminals went on to fight in World War II, under the governments' promise that it would remove criminal charges. This group within the criminal world were called the *suki* ('bitches').[82] War broke out between the traditionalists that did not cooperate with the government, and the collaborators. It is difficult to determine which group won, as there were already new generations of criminals who did not adhere to the criminal code at all.[83] Next to these (violent) criminal groups, two other actors are important in this milieu: the *tsekhoviki,* the entrepreneurs of the criminal world that produced and supplied goods illegally, and part of the Soviet Union's governing elite, the *nomenklatura,* that used their official power to enrich themselves and others around them. Criminal cases from the Soviet Union demonstrate the intricate connections between the criminal world and the political, sometimes up to the highest levels of ministerial power.[84] These three elements, criminal groups, shadow entrepreneurs and corrupt officials formed a 'diabolical troika', that would have an important role in the Soviet Union's transition to a capitalist economy.[85]

During the rule of Gorbachev, two policy changes were made that had a significant impact on the criminal world. First, the prohibition installed by Gorbachev made the criminal world the new supplier of booze and other legal and illegal goods that were hard to come by in the Soviet Union. Second, in 1988 it became possible to start small private enterprises with the law on Cooperatives, which gave way for illegal enterprises to become legal ones.[86] For example, the service of protection, or *krysha*

[80] Mark Galeotti, "The Vory" (Yale University Press Podcast, 2018), https://www.stitcher.com/podcast/yale-university-press-podcast/e/55006781.
[81] Galeotti.
[82] Serguei Cheloukhine, "The Roots of Russian Organized Crime: From Old-Fashioned Professionals to the Organized Criminal Groups of Today," *Crime, Law and Social Change* 50, no. 4–5 (2008): 361, https://doi.org/10.1007/s10611-008-9117-5.
[83] Cheloukhine.
[84] Cheloukhine, 364.
[85] Dina Siegel, "Russian Biznes in The Netherlands," 2002, 45.
[86] Galeotti, "The Vory."

('roof') that is offered or imposed by criminal groups, was transferred into the legal world by starting private security companies. Furthermore, the criminal world became more diverse, as new types of criminals appear. One of these types is the bandit, or 'violent entrepreneurs': they participate openly in society, with the use of force as their unique selling point.[87] This resulted in the easy and indiscriminate use of violence by Russian criminals; both in internal and external conflicts.

The end of the Cold War and the dissolution of the Soviet Union created even more opportunities for criminals: under president Yeltsin, crime flourished, despite Yeltsin's efforts to counter it.[88] In the process of privatisation of state-owned holdings, criminal organisations and former government officials cooperated to acquire these properties at absurdly low prices, which resulted in criminalised banks and businesses.[89] The most successful entrepreneurs in this process formed a new class of businessmen: the oligarchs. Some of them came from the Soviet *Nomenklatura,* transferring their executive power into control over the organisation, others came from a criminal background.[90] During the transition of the Soviet Union to a market economy, the legal and illegal world became intertwined to such an extent that this is essential to take into account when analysing the modern Russian criminal world and the role it plays in hybrid warfare. With this historic background of the development of the criminal world in Russia, the development of the modern criminal world can be analysed. Despite the major system change that takes place during the dissolution of the Soviet Union, there are still some historical elements of the criminal world that remain, and are therefore important to understand. The next paragraph will elaborate on how these elements survive the end of the Soviet Union and adapt to the new market economy.

### 5.2 Crime in modern-day Russia

Getting a clear overview of the Russian criminal world is difficult given the interconnected nature with the legal world. The clear distinction between *vory*, shadow entrepreneurs and state officials has blurred since the end of the Soviet Union. The following paragraph will therefore outline the Russian criminal landscape since the end of the Soviet Union.

*Organised Crime in Russia*

Territorially based criminal groups dominate the criminal sphere, but the rituals and status of the *vory* are still in place. Although the rules to become a *vor* have been loosened, the higher leaders of criminal groups can be 'crowned' as a *vor,* a ritual by which they enter the highest sphere of criminal groups in a region.[91] This group is often referred to as 'mafia', although Russian organized crime has a fundamentally

87 Vadim Volkov, "Who Is Strong When the State Is Weak : Violent Entrepreneurs in Post-Communist Russia," Russia at the End of the Twentieth Century, 1998, 12, https://web.stanford.edu/group/Russia20/volumepdf/Volkov.pdf.
88 Irina Abramova, "The Funding of Traditional Organized Crime in Russia," Economic Affairs 27, no. 1 (2007): 18–21, https://doi.org/10.1111/j.1468-0270.2007.00704.x.
89 James O Finckenauer, "The Russian 'Mafia,'" *Society Abroad*, 2004, 62; Louise I Shelley, "Post-Soviet Organized Crime: Problem and Response," *European Journal on Criminal Policy and Research* 3–4 (1995), 9.
90 Sergei Guriev and Andrei Rachinsky, "The Role of Oligarchs in Russian Capitalism," *Journal of Economic Perspectives* 19, no. 1 (2005): 139, https://doi.org/10.1257/0895330053147994.
91 Federico Varese, *The Russian Mafia: Private Protection in a New Market Economy* (Oxford: Oxford University Press, 2001), 177.

different structure than other mafias. It is not a tightly connected network, but rather a collection of criminal groups, who work either autonomously or have limited coordination.[92] These criminal groups do have a strong internal hierarchy: there is a leader at the top, with deputies of different sections beneath him; sections are formed by team leaders and soldiers. An organisation like this is called a *bratva* (brotherhood) or *brigada* (brigade).[93] There are many different estimates of the total size of these criminal communities, ranging from 32,000 to 120,000 active members.[94] However, most estimates are based on statistics from the Russian Ministry of the Interior (MVD), which do not seem as reliable when put under the scrutiny of reliability tests. For example, the MVD figures do not hold up when compared to crime statistics from other countries, making it difficult to give a definitive size.[95]

*Competition*

Apart from the Russian criminal groups, there is an array of Caucasian criminal groups that is often filed under the term of 'Russian organised crime'. These groups, such as the Chechens, Armenians, Azerbaijani and Georgians, are distinctly different from Slavic groups, with their own traditions, culture and language. Most of these groups compete with each other and cooperate when necessary. An exception to this are Chechen criminal groups, who do not accept the authority of the *vory v zakone* and operate independently.[96] Another competitor of the organised crime groups are the Cossacks: an East-Slavic, Russian-Orthodox Christian group. Due to their independent status in the Russian Federation, the Cossacks have more power and privileges in certain regions than other citizens, which makes them a powerful opponent of criminal groups. However, it has been reported that criminals have started to infiltrate Cossack groups, in order to profit from this power and semi-autonomous status, using it for criminal gain.[97]

*Globalisation*

Since the 1990s, Russian criminal groups expanded their operations outside the borders of Russia, which had become a lot easier since the end of the Soviet Union. Russian and Chechen gangs started to compete for the criminal authority over the Baltic underworld, accompanied by an explosion of violence.[98] This extreme situation led to a sharp increase in attention from governments and the media, and thereby a strong response in police and law enforcement agencies. As a result, Russian criminal groups operating abroad could not uphold their position, and many were eradicated or forced to move back to Russia. Some scholars suggest this high interest from governments and the public was actually an overcompensation; that there was little to no threat for most Western countries.[99] From 2000 onwards, Russian organised crime continued to spread worldwide, but more covertly, acting as intermediaries: an important role in criminal networks.[100] Intermediaries (also called

92 Abramova, "The Funding of Traditional Organized Crime in Russia."
93 Siegel, "Russian Biznes in The Netherlands," 51.
94 Siegel.
95 Anton Weenink, "The Russian Mafia: A Private Actor in International Relations?," in *Non-State Actors in International Relations* (Farnham: Ashgate Publishing Limited, 2001), 55.
96 Varese, *The Russian Mafia: Private Protection in a New Market Economy, 178*.
97 Varese, 180.
98 Mark Galeotti, "The Russian 'Mafiya': Consolidation and Globalisation," *Global Crime* 6, no. 1 (2004): 54–69, https://doi.org/10.1080/1744057042000297972.
99 Lydia S. Rosner, "The Sexy Russian Mafia," accessed June 16, 2020, http://orgcrime.tripod.com/russexy.htm.
100 Galeotti, "The Russian 'Mafiya.'"

'facilitators' or 'brokers') offer specialised services as financiers or organisers to different networks.[101] Intermediaries have an important network function: they connect potential partners, buyers and sellers, or employees.[102] However, despite their global reach, the size and impact of these groups is rather limited and not as spectacular as portrayed by the media in the 1990s.

*Relationship with the state*

An important shift in the post-Soviet criminal world is the presidency of Vladimir Putin, starting in 1999. From the start, Putin made it clear he would not accept criminal behaviour that challenged the state's authority; behaviour that could embarrass the state. However, he did not start a campaign against organised crime, although he has increased his control over the criminal world.[103] In 2019, an amendment made it possible to prosecute criminals if they admitted to be part of a criminal network.[104] This increased the pressure on the *vory*, as it is in their code that membership should be acknowledged when asked. A similar pressure is put on the oligarchs; Putin made the 'deal' the oligarchs could keep their (illegally gathered) fortune, if they would stay away from politics. The state would turn against those who did not adhere, which can have serious consequences: some currently live in exile, others were jailed.[105] This strategy of dealing with powerful actors in Russia, legal or illegal, demonstrates Putin's approach: cooperate, or else.

*Criminal activities*

The skillset of Russian criminal actors has expanded since the dissolution of the Soviet Union: the modern Russian criminal has access to a variety of tactics, with an increasing level of sophistication: "the ability to carry out complex, high-stakes (high risk, high return) crimes".[106] This level of sophistication can be more important than the size of a criminal group: a small number of high-skilled people can have a larger impact than a criminal group with a lower level of sophistication.[107] However, both levels are still relevant in the Russian criminal world. The 'traditional' criminal activities still play an important role, especially in organised crime. Activities such as extortion (*krysha),* violence/assassinations (guns for hire), trafficking of goods (drugs, alcohol, tobacco, natural resources), human trafficking and arms trade.[108]

---

[101] Anton Weenink, "General Crime Pattern Analysis Eastern Europe," *The Cambridge Handbook of Forensic Psychology*, no. October (2002): 159–65, https://doi.org/10.1017/cbo9780511730290.020.

[102] Damian Zaitch, "Bosses, Brokers and Helpers," in *The Extremes of Social Space: Ways of Thinking About Changes at the Top and the Bottom of Advanced Transatlantic Societies* (Amsterdam, 2002), 517.

[103] Galeotti, "The Russian 'Mafiya.'"

[104] "Russia's Feared Mafia Leaders in 'Shock' as Vladimir Putin Shows Who's Boss ," South China Morning Post, March 8, 2019, https://www.scmp.com/news/world/russia-central-asia/article/3001483/russias-feared-mafia-leaders-shock-vladimir-putin.

[105] Marshall I. Goldman, "Putin and the Oligarchs," Council on Foreign Relations, 2004, https://www.cfr.org/world/putin-oligarchs/p8018.

[106] James O. Finckenauer and Elin J. Waring, *Russian Mafia in America: Immigration, Culture, and Crime* (Boston: Northeastern University Press, 1998), 119.

[107] Siegel, "Russian Biznes in The Netherlands," 50.

[108] Anton Weenink and Franca van der Laan, "The Search for the Russian Mafia: Central and Eastern European Criminals in the Netherlands, 1989-2005," *Trends in Organized Crime* 10, no. 4 (2007): 66, https://doi.org/10.1007/s12117-007-9012-y.

*Economic crimes*

Apart from these traditional criminal activities, new criminal activities are increasingly incorporated in both traditional and 'new' criminal groups.[109] Economic crimes for example, are on the rise: recent investigations have uncovered large-scale, transnational money laundering practices, christened with intriguing names such as the Proxy Platform, the Russian Laundromat and the Azerbaijani Laundromat.[110] These investigations showcase the involvement of Russian banks, politicians and businessmen in intricate money laundering schemes with a worldwide span. However, the investigation of these cases is difficult, as the Russian government is reluctant to cooperate.[111] The cases however demonstrate how illegal Russian rubbles are transferred through various constructs into legal Euro's on a European bank account.[112] Russian banks play an important and sometimes even coordinating role in these affairs: the Russian investment bank *Troika Dialog* was the key player in the 'Troika Laundromat', a worldwide money laundering scheme that laundered money through Lithuanian banks.[113] The rise of economic crime does not only have economic consequences: in 2018, the UK's Foreign Affairs Committee concluded that the corrupt Russian assets connected to the Kremlin directly and indirectly support Putin's campaign to undermine the UK and its allies. The clear link between corruption and a wider Russian strategy, makes it therefore an important issue for the UK's national security.[114]

*Cybercrime*

Next to economic criminality, the number of cybercrime cases has risen exponentially over the years, as the cyber-domain becomes more and more important and embedded in society. Russian cybercriminals offer their services on well-protected fora that are easy to access, ranging from credit card data to cyberattack tools.[115] Because of this increasing supply, the prices for these services have gone done, lowering the threshold to access these services even more. That the impact of cybercrime is growing as well, was demonstrated last year, when the U.S. indicted two Russian men of the hacker group 'Evil Corp': a Russian hackers collective. According to the indictment, Evil Corp is 'the world's most harmful cybercrime group',

---

109 James Finckenauer and Yuri Voronin, "The Threat of Russian Organized Crime," Issues in International Crime, 2001.

110 "The Proxy Platform," OCCRP, 2011, https://www.reportingproject.net/proxy/en/the-proxy-platform; Bart Crezee, "Miljarden Dollars Aan Russisch Witwasgeld Belandden Op Nederlandse En Europese Rekeningen.," De Correspondent, 2017, https://decorrespondent.nl/6448/miljarden-dollars-aan-russisch-witwasgeld-belandden-op-nederlandse-en-europese-rekeningen-hoe-zit-dat-precies/1953713675056-2bee0fc5; Luke Harding, Caelainn Barr, and Dina Nagapetyants, "Everything You Need to Know about the Azerbaijani Laundromat," The Guardian, 2017, https://www.theguardian.com/world/2017/sep/04/everything-you-need-to-know-about-the-azerbaijani-laundromat.

111 OCCRP, "The Russian Laundromat Exposed ," March 20, 2017, https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/.

112 Crezee, "Miljarden Dollars Aan Russisch Witwasgeld Belandden Op Nederlandse En Europese Rekeningen."

113 Karlijn Kuijpers, "Nederlandse Banken Zijn Een Schakel in Russische Miljardenfraude ," *De Groene Amsterdammer*, March 3, 2019, https://www.groene.nl/artikel/nederlandse-banken-zijn-een-schakel-in-russische-miljardenfraude.

114 Foreign Affairs Committee, "Moscow's Gold: Russian Corruption in the UK," 2018, 27.

115 Mathew J Schwartz, "Why Russian Cybercrime Markets Are Thriving ," July 28, 2010, https://www.bankinfosecurity.com/russian-cybercrime-markets-are-thriving-a-8439.

responsible for hundreds of millions in losses worldwide.[116] Given the prominence and increasing importance of the cyber domain in today's world, this type of crime will probably expand in the future.

### 5.3 Russian criminal actors in the Netherlands

In the Netherlands, the end of the Soviet Union led to a big 'Russian mafia-scare': the topic was covered extensively in the media.[117] However, in the scientific and parliamentary committee-reports that followed, it was concluded that the threat of Russian organised crime to Dutch society was not as substantial as sometimes portrayed. After extensive research, the police team dedicated to the topic of criminals from Central and Eastern European countries ("KT-NON") concluded that there was no presence of the Russian mafia in the Dutch criminal world.[118] Incidentally, the Netherlands is used location for meetings between Russian criminal leaders; it is considered a safe zone by Russian gangsters.[119] There are criminals with a Russian background active in the Netherlands: the Dutch police services regularly report cases of human trafficking, smuggling of illegal goods and of cocaine, classifying it as a 'serious, sometimes major problem'.[120] Nevertheless, the stake of this group in the national crime-figures is small.

When looking at the perception of crime, an interesting contrast appears. In Dutch society, criminals operating outside the legal structures (e.g. drug trafficking, banditry) are mostly perceived as the 'real' criminals. However, the perception of crime in the Russian-speaking community in the Netherlands is distinctly different. This is important to take into account, as it gives a different perspective on the meaning of the terms 'crime' and 'criminals'. For the Russian-speaking community, drug traffickers and thieves are seen as the 'small' criminals. The real threat, in their perspective, is the 'tough mafia': the people that try to penetrate legal economic and political structures.[121] The type of crime that seems to fit this description best, is financial and corporate crime, often labelled under the umbrella term 'economic crime'. The issue with this type of crime however, is its complex character. Weenink and Van der Laan state that there are several interesting criminal cases in this domain, but the complexity of these cases makes it difficult to resolve them.[122] Additionally, of the thousands of suspicious transactions reported in the Netherlands, very few are made into a criminal case; government institutions are lacking either the resources or the capabilities to do so.[123] Given the lack of information and evidence

[116] "Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of 'Bugat' Malware ," US Department of Justice, December 1, 2019, https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens.
[117] Siegel, "Russian Biznes in The Netherlands," 9.
[118] Anton Weenink and Franca van der Laan, "The Search for the Russian Mafia: Central and Eastern European Criminals in the Netherlands, 1989-2005," *Trends in Organized Crime* 10, no. 4 (2007): 75, https://doi.org/10.1007/s12117-007-9012-y.
[119] Siegel, "Russian Biznes in The Netherlands."
[120] Weenink, "General Crime Pattern Analysis Eastern Europe."
[121] Siegel, 180.
[122] Weenink and van der Laan, "The Search for the Russian Mafia: Central and Eastern European Criminals in the Netherlands, 1989-2005."
[123] Dirk Waterval, "Tienduizenden witwasmeldingen, amper strafzaken. 'Soms lijkt het of het hele meldsysteem voor niets is,'" *Trouw*, July 27, 2020,

of these practices, it is difficult to get a good understanding of the scale and impact of economic crimes in the Netherlands, which makes it all the more important to take this uncertainty into account in scenario building. Before the scenario-building phase however, the topics of Russian hybrid warfare and criminal actors are connected in the following paragraph. Building on the extensive study of these topics separately, a first image of the role of criminal actors in hybrid warfare can be developed.

### 5.4 Criminal actors in the Russian concept of hybrid warfare

When looking at the participation of criminal actors in Russian hybrid warfare, several cases can be identified in three different domains: violent conflict, cybercrime and arms trafficking.

First, the most striking cases are in the violent conflicts Russia has engaged in over the years. During the Georgian-Russian war in 2008, criminals played a significant role. Ethnic-Georgian villages were looted by criminal gangs and militia, thereby forcing the Georgian population out of the region.[124] Before and during the Russian annexation of Crimea, the strong connections between criminal groups and the Russian government were used to consolidate the Russian grip on the region.[125] In the current conflict in Eastern Ukraine, Russian services have formed militias from volunteers, mercenaries, criminals and defectors in the fight against the Ukrainian government.[126] It seems that this use of criminal actors is mostly opportunistic for the Russian government: it gives more manpower, in a quick and efficient manner. For criminals, it can be beneficiary at the same time: they can use the 'fog of war' to continue or even expand their activities, while at the same time improving their fighting skills.

Perhaps the most 'visible' use of criminals by the Russian government is in the cyber domain. Cybercriminals were active in the conflicts in Georgia and Ukraine, but were also used in various cyberattacks on governments, infrastructure and businesses: for example in the DDoS attack on Estonia in 2007, or the leaked emails in the US and French elections.[127] Often, the hackers involved are not directly part of the Russian government, but are recruited for a specific task, the so-called 'patriotic hackers'. Another method of recruitment, is offering arrested cybercriminals the choice between prison or cooperation with the FSB, where the latter includes protection from other governments; an offer that seems hard to refuse.[128] Additionally, there seem to be links between the Russian government and 'normal' cybercriminals: in the indictment of the beforementioned hacker group 'Evil Corp', the U.S. Treasury accuses the subjects of the indictment of working for the FSB since 2017 and tasked

https://www.trouw.nl/economie/tienduizenden-witwasmeldingen-amper-strafzaken-soms-lijkt-het-of-het-hele-meldsysteem-voor-niets-is~b03c7f64/.

[124] Thomas Hammarberg, "Human Rights in Areas Affected by the South Ossetia Conflict," *Commissioner for Human Rights*, 2008.

[125] Mark Galeotti and Radio Free Europe, "Crime And Crimea: Criminals As Allies And Agents," Radio Free Europe, n.d., https://www.rferl.org/a/crimea-crime-criminals-as-agents-allies/26671923.html.

[126] Galeotti, "Hybrid, Ambiguous, and Non-Linear?"

[127] Tim Maurer, "Cyber Proxies on the Loose: The Former Soviet Union," *Cyber Mercenaries*, 2017, 97, https://doi.org/10.1017/9781316422724.007.

[128] Maurer, 96.

with acquiring confidential documents through its cyber operations. The Treasury did not elaborate on this accusation, however.[129]

The method of working together with individuals with specific skills does not only occur in relation to cybercrime: this happens in arms trade as well, with the Russian arms trafficker Viktor Bout as the most famous example. Bout built up a cargo fleet of airplanes, which he then used to transport arms to governments and independent groups all over the world. In 2008, Bout was arrested in an undercover operation by the DEA, and extradited in 2010 to the U.S.[130] During his 'career', Bout had some protection from the Russian government; he developed close relations with high Russian officials and rushed to his home country when threatened. After his arrest, Russian officials spoke out against his case, in favour of Bout, and extradition to Russia was requested.[131]

Apart from the cases where the cooperation between criminal actors and the Russian government is evident, there are several categories where this is suspected, or likely to have happened given the extensive use of non-state actors by the Russian government and the interconnected nature of legal and illegal businesses in Russia. These three different categories are outlined below.

*Violence*

Over the last few years, several assassinations have taken place in Europe, for example the poisoning of Aleksandr Litvinenko and Sergei Skripal, or assassinations that targeted Chechen dissidents, likely ordered by Putin's strongman Ramzan Kadyrov.[132] The evidence in most of these cases points to Russian intelligence-operatives as being responsible for these murder (attempts), despite the Russian rejection of this evidence.[133] However, this is not clear for all cases: in some, a connection with criminal actors is suspected: for example in doing the 'ground work' for these operations.[134] A recent investigation by Bellingcat connected a Russian criminal to a recent assassination in Berlin; this is however not yet confirmed by a verdict in a criminal case.[135]

[129] "Russian 'Evil Corp' Hackers Charged by US in $100m Cyber Theft ," Al Jazeera, August 6, 2019, https://www.aljazeera.com/news/2019/12/russian-evil-corp-hackers-charged-100m-cyber-theft-191206054758063.html.
[130] "Trapping the Lord of War: The Rise and Fall of Viktor Bout ," Der Spiegel International, October 6, 2010, https://www.spiegel.de/international/world/trapping-the-lord-of-war-the-rise-and-fall-of-viktor-bout-a-721532.html.
[131] "Trapping the Lord of War: The Rise and Fall of Viktor Bout ."
[132] Robyn Dixon, "Chechen Exiles Are Being Hunted down. Often, the Trail Leads Back to Russia," *The Washington Post* , July 4, 2020, https://www.washingtonpost.com/world/europe/chechen-exiles-are-being-hunted-down-often-the-trail-leads-back-to-russia/2020/07/06/e16d9e12-bf68-11ea-864a-0dd31b9d6917_story.html.
[133] "The GRU Globetrotters: Mission London ," Bellingcat Investigation Team, June 28, 2019, https://www.bellingcat.com/news/uk-and-europe/2019/06/28/the-gru-globetrotters-mission-london/.
[134] Mark Galeotti, "Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe," *The Oxford Handbook of Organized Crime*, no. January (2014): 1–12.
[135] Bellingcat, "Identifying The Berlin Bicycle Assassin: From Moscow to Berlin ," December 3, 2019, https://www.bellingcat.com/news/uk-and-europe/2019/12/03/identifying-the-berlin-bicycle-assassin-part-1-from-moscow-to-berlin/.

*Intermediaries*
Given the role of Russian criminal actors as intermediaries in the global underworld, it is possible that government services could make use of this role as well in European countries. A local criminal network could provide intelligence officers easier access to a country, for example.

*Economic crime*
The strong connections between the Russian legal world and the criminal world make it relatively easy for the Russian government to profit from, or use economic crime. This would be beneficial if certain money flows have to be hidden from the public, or if a government actor wants to avoid sanctions. Given the complex and global nature of this type of criminal cases, it is difficult to address this problem. At the same time, economic crimes can be used aggressively as well, as it would enable the Russian government to disrupt economic processes in the targeted country.

*Characterising criminal actors in hybrid warfare*
Looking at past and suspected cases is not enough to get a comprehensive insight into this practice: a more structured approach is desirable. In the overview by RAND, (figure 1) the only criminal actors mentioned are cybercriminals. This is often the case in research into actors in hybrid warfare. On the theoretical level, a vast array of possible actors is mentioned, but only the most common examples of actors are studied in-depth. The models introduced in the fourth chapter are therefore used to conceptualise the relationship and function of criminal actors.

The model by Maurer (figure 2) is used to characterise the relationship between the proxy and the state. The most common relationship between criminal actors and the Russian government can be categorised as type II (state/non-state): criminal actors are the proxy, the Russian government the beneficiary. An example of this relationship is the use of criminals in violent conflict, for example in Ukraine. However, type III (non-state/state) could apply as well. Although the top level of the Russian government has absolute authority on state matters, the interconnected nature of legal and illegal businesses makes it difficult to distinguish between type II and III proxy relationships. The focus however will be on type II: the threat of a proxy relationship between the Russian state as the beneficiary and Russian criminal actors as the proxy.

To study the function of criminal actors in hybrid warfare, the model of Rauta (figure 3) is used. Firstly, the relational embeddedness of criminal actors is indirect: criminal actors are not directly embedded in Russian forces, but operate apart from government entities. Second, the relational morphology can be both supplementary and delegatory. To take cyberattacks as an example: the attack on Estonian infrastructure in 2007 was delegatory; the task at hand was delegated to cybercriminals and not part of a larger attack. The cyberattacks on Georgia however, was supplementary to the larger coordinated attack by Russian forces, the first time that there has been a coordinated cyber component to an international conflict.[136] This gives criminal actors in hybrid conflict therefore two possible functions: as a surrogate (indirect, supplementary) or as a proxy (indirect, delegatory).

[136] Maurer, "Cyber Proxies on the Loose: The Former Soviet Union," 101.

The beforementioned examples of the suspected cooperation between criminal actors and the Russian government demonstrate the two functions that are introduced in the paragraphs above. The functions of criminal actors are either as a surrogate (cybercrime, violence in conflicts, intermediaries) or as a proxy (assassinations, cybercrime, economic crime). However, these functions can change: criminal actors can have multiple functions simultaneously. This classification gives a better understanding of the role of criminal actors in hybrid warfare, as it identifies the dynamics of the state/non-state relationship. At the same time this classification has its limits, given the fluid character of this relationship. This will be taken into account in the next chapter, in which scenarios are developed on the threat of criminal actors in the Netherlands.

# 6 Driver analysis

The goal of this thesis is to provide an insight into the threat posed by Russian criminal groups as an instrument of the Russian government, specifically for the Netherlands. After outlining the current state of the Russian government and Russian criminal organisations, an insight into future developments can be formed. The following chapters address the last two sub-questions, which look at how the role of criminal actors in hybrid warfare role can be detected and how this role of these actors in the Netherlands can develop in the future. This is done by developing scenarios and indicators.

Scenarios are not developed from the creative thinking of the author, but in structured manner. First, the drivers are identified:  the deepest level of the analysis of a certain topic. There are two main categories: drivers on actors and drivers on factors. The first category is identified using a SWOT analysis: a framework that analyses an actor's strategic position by looking at the strengths, weaknesses, opportunities and threats of this actor. The second category, drivers on factors is identified using a Causal Loop Diagram (CLD). This is a diagram that visualises causal relations between variables in a system, which creates an overview of the different factors and dynamics in play. From these causal relations and the SWOT analyses, drivers can be derived using logic reasoning.  Both methods take the perspective of the Russian government, identifying possible drivers of the Russian government's actions regarding hybrid operations and the use of criminal actors.

Next, the drivers are ranked on their level of uncertainty and impact. The lower the uncertainty score, the more certain it is that the specific dynamic/driver will occur, and vice versa.  The level of impact is the measure of a driver's impact on society; the higher the score, the more impact it would have. The drivers are then compared in a paired ranking, which identifies the highest-scoring drivers. From these key drivers, the two core uncertainties are generated, which lead to four different scenarios, indicating four different pathways of how the relationship between criminal actors and hybrid operations could develop. These scenarios are extended with indicators, which provide signals of whether or not a scenario is unfolding.

## 6.1 SWOT-analysis

| Strengths | Weaknesses |
|---|---|
| – Good connections with neighbouring EU countries<br>– Strongly integrated in NAVO<br>– Well-functioning democracy<br>– Easy to access; open borders<br>– Effective law enforcement agencies | – Economic effects of COVID-19<br>– Open society, vulnerable for outside influence<br>– Slow government response due to democratic systems<br>– Dependent on Russian energy supply |
| **Opportunities** | **Threats** |
| – Growing economy<br>– Solidify position in EU after Brexit<br>– Improve position as a trade hub / transit country | – Polarization in society<br>– Unrest in partnerships (i.e. Brexit) |

### *6.1.1 SWOT The Netherlands*

From a Russian perspective, the Netherlands is an important country in Europe, despite its small size. It has a strong economy and is well-integrated in the EU and NAVO, which gives the country a significant diplomatic and militarily profile. Furthermore, it is has a growing and open economy, and an important position as a trade hub in the world economy.

By cross-referencing the different elements of this SWOT and using logical reasoning, several drivers can be identified: key motives in the relationship of the two countries, from the Russian perspective.

- Though open borders and an accessible economy are strengths of the Netherlands, this openness could also provide access to actors such as the Russian government. There are two possible explanations for the Russian government to do so: either to access the European market (DA1), or to access neighbouring EU countries (DA3).
- Furthermore, the sanction regime and the energy supply are two key topics for the Russian government regarding the Netherlands. The sanction regime has had a large negative impact on the Russian economy and is supported by the Netherlands, among others. A change in the Dutch perspective is therefore an important driver, certainly given the country's embeddedness in the EU and NATO. (DA4)
- Lastly, the Dutch dependency on Russian energy is an important driver between these states, as it makes the Dutch state quite dependent. Reducing this dependency would change Russia's political power over the country (DA2). The drivers from this SWOT are listed below.
–

**Drivers**

| | |
|---|---|
| DA1 | The Russian government gains access to the European market via the Netherlands |
| DA2 | The Dutch government diversifies its energy supply |
| DA3 | The Russian government has access to neighbouring countries via the Netherlands |
| DA4 | The Dutch perspective on the sanction regime on Russia changes |

### *6.1.2 SWOT Russian Federation*

| **Strengths** | **Weaknesses** |
|---|---|
| – Large amounts of natural resources<br>– Powerful military<br>– Power over energy supply; other countries dependent on Russia<br>– Influence over former Soviet states<br>– Strong grip on internal actors in the political domain (organisations & institutions) | – Sanctioned by Western countries<br>– Strong dependency on energy market & prices<br>– Corruption in government and businesses |
| **Opportunities** | **Threats** |
| – Economic and military growth of ally China<br>– Opening up of Northern naval route<br>– Societal & political unrest among adversaries (US, EU) | – Increasing public unrest<br>– Growing dependency on China<br>– Enlargement of NATO<br>– Increasing scrutiny from open-source investigations, journalists |

The Russian Federation is one of the major players on the geopolitical stage: it has a powerful military apparatus, large natural resources and a strong grip on internal actors. However, it is under pressure from different sides: societal unrest is increasing and the country is economically in dire straits due to its dependence on the energy market and the imposed sanction regime. While the growth of China can be beneficial to Russia, it is at the same time a threat, as it could make the country more dependent on China.

Using cross-referencing and logical reasoning, several drivers can be identified that play a role in the topic of this study.

- First, the Russian government can use its strong grip on internal actors in the political domain to obtain its political goals. This is expressed in the first driver, DA5.
- The second relevant driver deals with the Russian energy supply. Does many countries depend on Russia for their energy supply, the Russian government has extensive power in this domain, which it can use as leverage. This economic and political instrument is therefore vital in the country's geopolitical position and therefore driver DA6.
- Russian internal affairs play an important role in this matter. Despite the government's aggressive conduct towards the political opposition, social unrest lingers. This could have a negative impact on the country's ability to achieve its external political goals, which makes preventing further escalation of internal unrest an important driver (DA7).
- Lastly, the country is under a sanction regime from Western countries after the annexation of Crimea, which puts a heavy strain on the country's economy. There are two ways in which the country can deal with this sanction regime. First, it can avoid sanctions by operating covertly, minimising the risk of new sanctions as a result of hybrid operations (DA8).
- However, Russian operations have become more exposed as a result of the open-source investigations from researchers and journalists across the world. Although the Kremlin structurally denies the allegations made by these open-source investigations, the worldwide attention it culminates makes foreign operations a lot more challenging. Second, The Russian government can try to

change the sanction regime by more diplomatic means. given the impact the sanction regime has, this is of major concern to the Russian government (DA9).

**Drivers**

| | |
|---|---|
| DA5 | The Russian government uses its strong grip on internal actors (organisations / institutions) for its foreign political goals |
| DA6 | The Russian government uses other countries' energy dependency on Russia as leverage |
| DA7 | The Russian government prevents social unrest in society |
| DA8 | Russia avoids more sanctions by operating covertly |
| DA9 | The sanction regime is cancelled |

### *6.1.3 SWOT Russian criminal actors*

| **Strengths** | **Weaknesses** |
|---|---|
| – Spread over Russia<br>– Interconnected with Russian legal economy, strong influence on business<br>– Large skillset<br>– International network | – No clear chain of command; loosely connected networks<br>– Rivalry between criminal groups and other groups (i.e. Cossacks) |
| **Opportunities** | **Threats** |
| – Cooperation with criminal groups worldwide<br>– Extending influence in society as a result of COVID-19<br>– Cooperation with Russian state services | – Increasing pressure from police<br>– Increasing pressure from international police investigations (Interpol, Europol)<br>– Internal competition |

There is no archetype of a Russian criminal actor; they do not operate as a single entity. The strengths, weaknesses, opportunities and threats therefore do not necessarily apply to every criminal actor, but most apply to the different types of criminal actors. In general, Russian criminal actors have a powerful presence in Russia; possessing a large skill set and are able to operate across the globe through their international network.

Cross-referencing these components leads to the following drivers:

- As with normal businesses, the goal is to increase the market share in the illicit economy. The COVID-19 crisis in particular created opportunities for criminal actors, as they can use the economic downfall and improve their popularity among society at the same time (DA10).[137]
- In order to avoid or reduce the pressure from police investigations, developing cooperation with the Russian government and state officials could benefit both government and criminal actors. A better relationship with the state and mutual interests in this cooperation, is likely to improve the cover provided by the Russian state in international crimefighting efforts; as several notorious (cyber) criminals have demonstrated. This dynamic therefore leads to DA11.
- An important characteristic of the criminal world, is its highly competitive nature. However, internal conflicts often have a negative effect on the parties involved due to the costs of conflicts and an increasing police attention. Reducing internal competition will therefore benefit Russian criminal actors (DA12).
- In line with DA11, there are certain advantages to run on international criminal operations from Russia. Given the country's reluctance to cooperate in international police investigations, it offers some protection.[138] Furthermore, the emigration of criminal organisations increases investigative efforts from the police, as is demonstrated in the past. The use of Russia as a home base is therefore the last driver from this SWOT analysis (DA13).

[137] "How Mexican Cartels Are Gaining from Covid-19 ," BBC News, July 10, 2020, https://www.bbc.com/news/av/world-latin-america-53343599/coronavirus-how-mexican-cartels-are-taking-advantage-of-pandemic; Sofia Bettiza, "Coronavirus: The Lure of Mafia Money during the Crisis ," BBC News , May 5, 2020, https://www.bbc.com/news/world-europe-52537573.

[138] The Russian government often refuses to cooperate with international criminal investigations, especially on high-profile cases such as MH17 or the Skripal case.

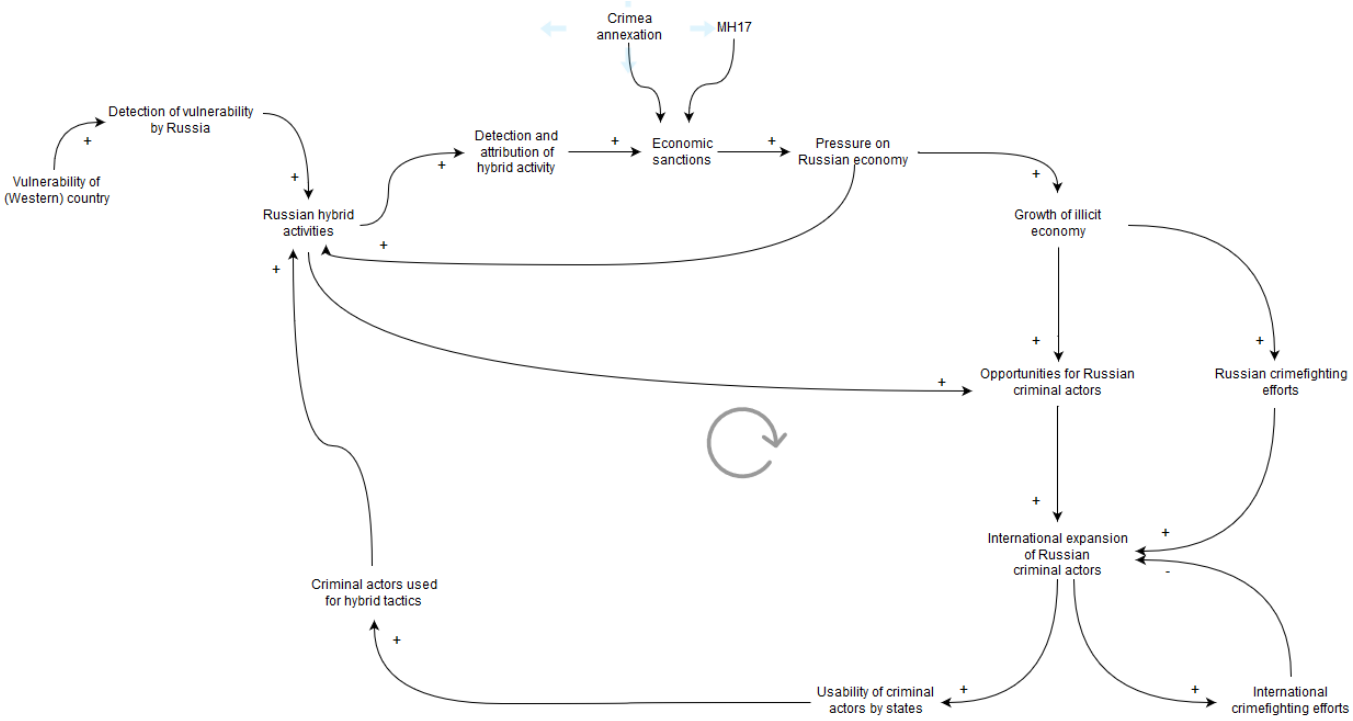
**Drivers**

| | |
|---|---|
| DA10 | Russian criminal actors expand their position in the (international) shadow economy |
| DA11 | Russian criminal actors cooperate with the Russian state to counter international crimefighting efforts |
| DA12 | Cooperation among Russian criminal actors is increased to reduce internal competition |
| DA13 | Russia is used as a home base for international criminal activities to avoid international police investigations |

## 6.2 Causal Loop Diagram

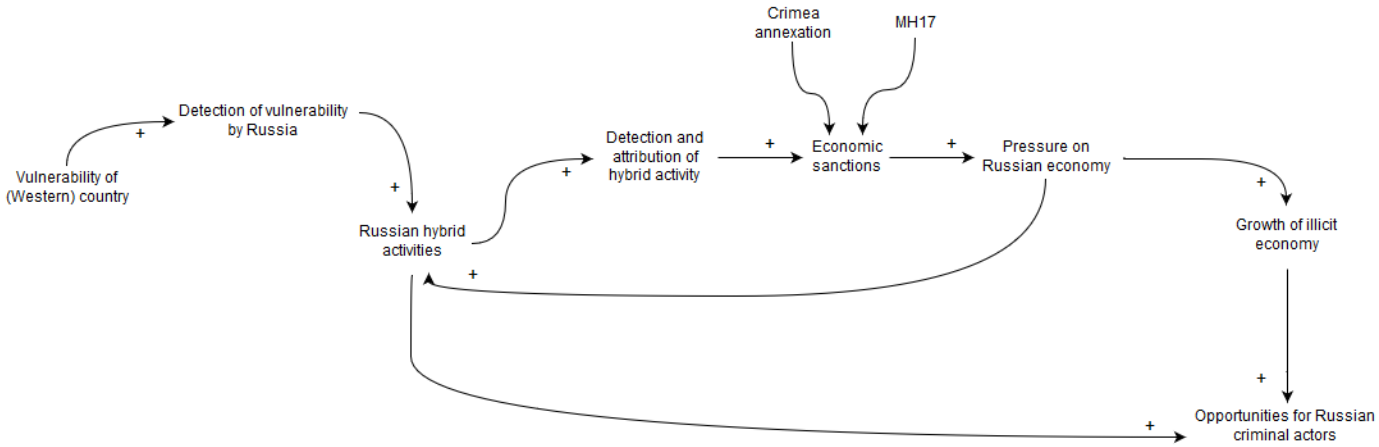
The actor analysis with the SWOT framework gives an overview of the drivers from the perspective of the actors. Next, another exploratory technique is used to get an insight into the drivers: the causal loop diagram. This technique focuses on drivers on the factor-level, studying the dynamics that are at play in a domain. The drivers that are generated from the causal loop diagram form, together with the drivers from the SWOT analysis, the basis for the scenarios after a paired ranking of all drivers. Below, the full diagram is introduced and explained, followed by an explanation of the subloops.

### *6.2.1 Full diagram*




This diagram shows what can lead to the use of criminal actors for Russian hybrid activities and which dynamics can play a role. Hybrid activities are often aimed at a vulnerability in a country that is the target of a hybrid operation. Although it is difficult to identify a conclusive Russian motive for these operations, the beforementioned worldview of Russia as a global superpower and the fear of Western expansion or domination, likely plays an important role.

*6.2.2 Hybrid activities to opportunities via sanctions*




If hybrid activities are detected and attributed by the target, consequences will follow. After the annexation of Crimea for example, the U.S. and other Western countries put a number of sanctions on Russia, which are still in place.[139] Especially economic sanctions can have large impact on a country: it is estimated the Russian economy lost 1% of its annual GDP after the first year of sanctions.[140] This economic pressure creates opportunities for criminal actors; for example in trading sanctioned goods. A different pathway is however possible; hybrid activities in general can create more opportunities for criminal actors; either by cooperating with the government in certain activities (for example in the conflicts in Ukraine) or by profiting from being less of a priority for the government.

In this subloop, the drivers are the interventions that ultimately lead to the result of this loop: opportunities for Russian criminal actors. These are the following:

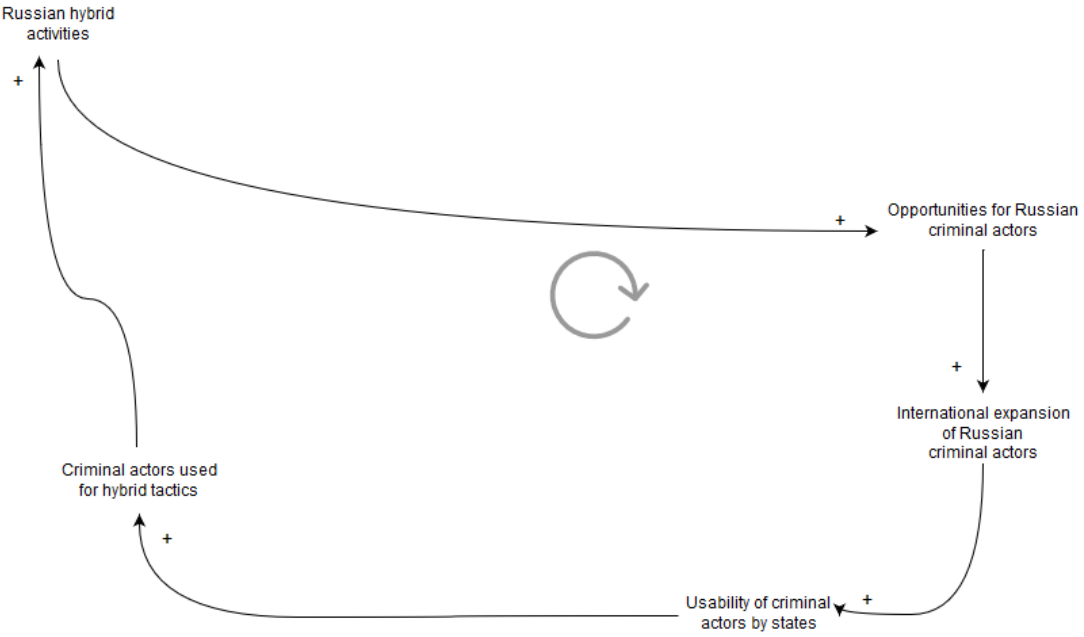
- In order to undertake hybrid activities, a vulnerability has to be detected and targeted by an adversary. This is the first driver, DF1.
- Second, these hybrid activities have to be detected and attributed to continue this loop: without either of these aspects, no action can be taken in response (DF2)
- In response to hybrid activities, sanctions are implemented. There are different types of sanctions: economic (on goods or industries), personal (on specific persons), or diplomatic: after the Skripal poisoning, a large number of countries expelled their Russian diplomats in support of the UK.[141] Often, a combination of these different types of sanctions is applied (DF3).
- In this causal loop diagram, the focus is on economic sanctions, as they are the most relevant regarding the focus on criminal actors. Criminal actors have the ability to circumvent the official channels, thereby creating the opportunity to avoid sanctions and continue the trade in sanctioned goods, which expands the illicit economy (DF4).

[139] "U.S. Sanctions on Russia," January 17, 2020, https://fas.org/sgp/crs/row/R45415.pdf.
[140] Peter Havlik, "EU-Russia Sanctions Exchange Has Had Important Economic and Political Consequences," February 20, 2019, https://wiiw.ac.at/n-365.html.
[141] Angela Dewan, Milena Veselinovic, and Carol Jordan, "All the Countries Expelling Russian Diplomats," *CNN*, March 28, 2018, https://edition.cnn.com/2018/03/26/europe/full-list-of-russian-diplomats-expelled-over-s-intl/index.html.

**Drivers**

| | |
|---|---|
| DF1 | A country’s vulnerability is detected and targeted |
| DF2 | Hybrid activities are detected and attributed |
| DF3 | Sanctions are implemented as a result of hybrid activity |
| DF4 | Economic sanctions cause an expansion of the illicit economy |

### *6.2.3 Opportunities leading to use of criminal actors*




Next, growing opportunities can lead to (further) international expansion: larger criminal networks are more able to operate internationally. An international network of Russian criminal actors makes them more usable for hybrid activities, which increases the chance of criminal actors being used by the government. The drivers behind this usability are twofold:

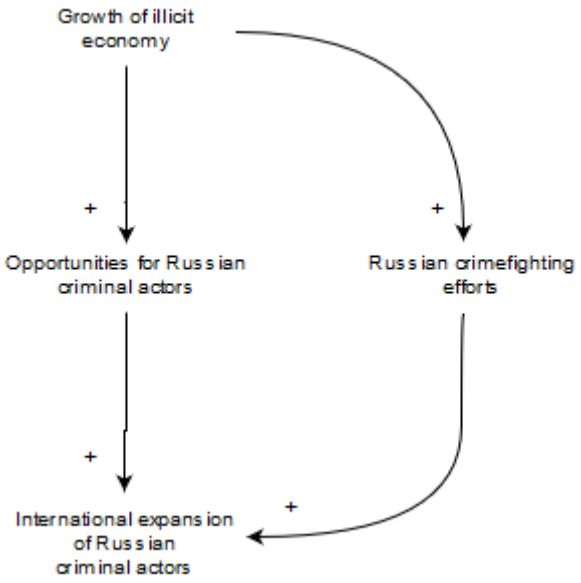
- First, criminal networks could give state services easier access to a country's economy and society in hybrid operations, as there is already a network present in the country (DF5).
- Second, the criminal routes for goods (smuggling) or money (money laundering) between Russia and other countries could be used as a 'shadow highway' by the government, for example in trading sanctioned goods (DF6).[142]

**Drivers**

| | |
|---|---|
| DF5 | Russian criminal actors' networks are used as a point of entry for hybrid activities |
| DF6 | Physical and digital routes used by Russian criminal actors are used by the Russian government |

[142] Mark Galeotti, "Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe," *The Oxford Handbook of Organized Crime*, no. January (2014): 5.

### *6.2.4 International expansion of Russian criminal actors*



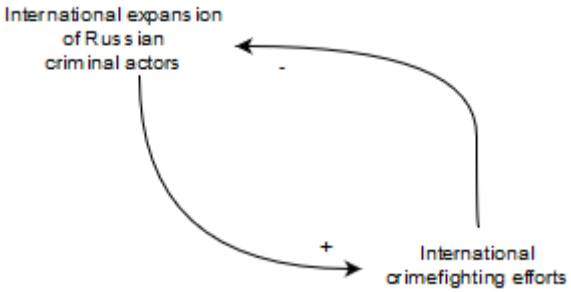

A growing illicit economy has positive and negative effects on criminal actors. On the one hand, it increases the opportunities for criminal actors. On the other hand, it can trigger a stronger police effort to counter crime. Although the Russian police is plagued by corruption and a declining trust from the public, crime numbers have been declining since 2002.[143] If it becomes too difficult for criminal actors to operate on Russian soil, the increasing pressure from the police can result in a migration of criminal activities, as has happened in the past.[144] Both dynamics can contribute to an international expansion of criminal actors and are therefore the drivers: either international expansion comes about by a growing illicit market (DF7) or as a way to avoid Russian crimefighting efforts (DF8).

**Drivers**

| | |
|---|---|
| DF7 | The Russian criminal actors expand globally due to a growing illicit market |
| DF8 | Russian criminal actors avoid Russian crimefighting efforts by going global |

[143] "Russia Crime Rate & Statistics 1990-2020," Macrotrends, 2020, https://www.macrotrends.net/countries/RUS/russia/crime-rate-statistics.
[144] Federico Varese, "The Structure and the Content of Criminal Connections: The Russian Mafia in Italy," *European Sociological Review* 29, no. 5 (2013): 900, https://doi.org/10.1093/esr/jcs067.

### *6.2.5 Expansion and crimefighting*




International expansion of Russian criminal actors will however also lead to an international response from police and security services. This response can come from the country where the criminal actors have migrated to, but more and more, criminal actors are countered by transnational efforts, coordinated by institutions such as Europol.[145] There are two drivers behind this interplay of crimefighting and criminal expansion:

- In order to avoid international crimefighting efforts, Russian criminal actors operate mostly from Russia (DF9).
- Crimefighting efforts can put a lot of pressure on the international expansion of criminal actors and ultimately even force them out of a country or region, as happened in the Baltic states after the wave of Russian crime in the 1990s.[146] This disturbing effect of international crimefighting can have a large impact on how criminal actors spread (DF10).

**Drivers**

| | |
|---|---|
| DF9 | Russian criminal actors avoid international crimefighting efforts by operating from Russia |
| DF10 | International crimefighting efforts disturb international expansion of Russian criminal actors |

[145] Ivana Saric, "Europol Helps Break Up Two Smuggling and Trafficking Gangs," OCCRP, June 18, 2019, https://www.occrp.org/en/daily/9987-europol-helps-break-up-two-smuggling-and-trafficking-gangs; "Two Main Russian Mafia Groups Dismantled in Spain with Europol's Support," Europol, August 28, 2017, https://www.europol.europa.eu/newsroom/news/two-main-russian-mafia-groups-dismantled-in-spain-europol's-support.
[146] Galeotti, "The Russian 'Mafiya.'"

## 6.3 Drivers

From the SWOT analysis and the CLD, a list of drivers is derived that will be used as a basis for the scenarios. However, not all drivers can be used for scenarios; that would generate too many possibilities. The drivers will therefore be ordered on uncertainty and impact, and then ranked. The highest-ranking drivers are the core uncertainties on which the scenarios will be based. The drivers are ranked on a scale from 1 to 10; 1 being the lowest value and 10 the highest. Although these scores are based on the extensive literature study of this thesis, the assessment of these values is a subjective process. To minimalize this subjectivity, this ranking is reviewed by the thesis supervisors.

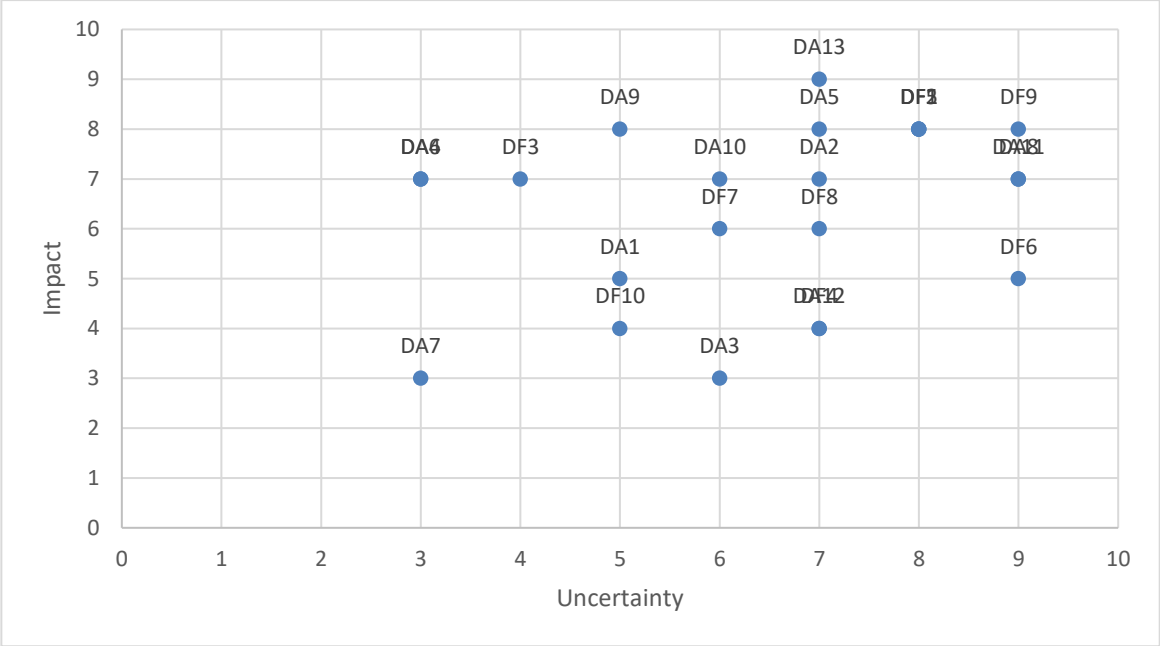
*6.3.1 List of drivers & ranking*

| **Drivers on actors** | | **Uncertainty** | **Impact** |
|---|---|---|---|
| DA1 | The Russian government gains access to the European market via the Netherlands | 5 | 5 |
| DA2 | The Dutch government diversifies its energy supply | 7 | 7 |
| DA3 | The Russian government has access to neighbouring countries via the Netherlands | 6 | 3 |
| DA4 | The Dutch perspective on the sanction regime on Russia changes | 3 | 7 |
| DA5 | The Russian government uses its strong grip on internal actors (organisations / institutions) for its foreign political goals | 7 | 8 |
| DA6 | The Russian government uses other countries' energy dependency on Russia as leverage | 3 | 7 |
| DA7 | The Russian government prevents social unrest in society | 3 | 3 |
| DA8 | Russia avoids sanctions by operating covertly | 9 | 7 |
| DA9 | The sanction regime is cancelled | 5 | 8 |
| DA10 | Russian criminal actors expand their position in the international shadow economy | 6 | 7 |
| DA11 | Russian criminal actors cooperate with the Russian state to counter international crimefighting efforts | 9 | 7 |
| DA12 | Cooperation among Russian criminal actors is increased to reduce internal competition | 7 | 4 |
| DA13 | Russia is used as a home base for international criminal activities to avoid international police investigations | 7 | 8 |

| **Drivers on factors** | | **Uncertainty** | **Impact** |
|---|---|---|---|
| DF1 | A country's vulnerability is detected and targeted | 8 | 8 |
| DF2 | Hybrid activities are detected and attributed | 8 | 8 |
| DF3 | Sanctions are implemented as a result of hybrid activity | 4 | 7 |
| DF4 | Economic sanctions cause an expansion of the illicit economy | 7 | 4 |

| | | | |
|---|---|---|---|
| DF5 | Russian criminal actors' networks are used as a point of entry for hybrid activities | 8 | 8 |
| DF6 | Physical and digital routes used by Russian criminal actors are used by the Russian government | 9 | 5 |
| DF7 | The Russian criminal actors expand globally due to a growing illicit market | 6 | 6 |
| DF8 | Russian criminal actors avoid Russian crimefighting efforts by going global | 7 | 6 |
| DF9 | Russian criminal actors avoid international crimefighting efforts by operating from Russia | 9 | 8 |
| DF10 | International crimefighting efforts disturb international expansion of Russian criminal actors | 5 | 4 |

*6.3.2 Impact x uncertainty matrix*




*6.3.3 Key drivers*

The paired ranking can be found in the appendix. The highest-ranking drivers are:

DA5 The Russian government uses its strong grip on internal actors (organisations/institutions) for its foreign political goals
DA8 Russia avoids sanctions by operating covertly
DA11 Russian criminal actors cooperate with the Russian state to counter international crimefighting efforts
DF1 A country's vulnerability is detected and targeted
DF2 Hybrid activities are detected and attributed
DF5 Russian criminal actors' networks are used as a point of entry for hybrid activities
DF9 Russian criminal actors avoid international crimefighting efforts by operating from Russia

# 7 Scenarios

Building on the understanding of criminal actors, the concept of hybrid warfare in Russia and the identified drivers of these actors, several scenarios are developed. The aim of this exercise is twofold: first, it gives a perspective on possible developments in the future. Second, the indicators improve the ability to monitor for this type of threat. More specifically, policymakers can prepare for this type of hybrid actor, as it gives an indication of the threat level for the Netherlands. Finally, it improves the understanding of this phenomenon, making it clearer where to look, and what to look out for.

From the driver analysis and the paired ranking, certain trends are generated: drivers that score low on uncertainty and high on impact: these are therefore likely to occur in the near future. The trends are DA6 (The Russian government uses other countries' energy dependency on Russia as leverage) and DF3 (Economic sanctions cause an expansion of the illicit economy). The Kremlin has used its power over the energy supply for political power in the past, especially in disputes with countries surrounding Russia. This can have consequences for the energy supply of European countries as well, naturally. The second trend, economic sanctions cause an expansion of the Russian illicit economy, is more difficult to observe. However, as sanctions are often put on specific goods that cannot be easily replaced by a country's own production, this consequence is likely to follow.

From the driver analysis, two core uncertainties can be distilled, by looking at common themes or overlap in the key drivers identified in paragraph 6.3.3. The following key drivers can be grouped:

DA5 The Russian government uses its strong grip on internal actors for its foreign political goals
DA11 Russian criminal actors cooperate with the Russian state to counter international crimefighting efforts
DF5 Russian criminal actors' networks are used as a point of entry for hybrid activities.

These three drivers focus on whether or not there is a form of cooperation between the Russian state and Russian criminal actors, either voluntary or involuntary. Furthermore, this cooperation is essential in analysing the role of criminal actors, making it therefore a core uncertainty. The second grouping of drivers is focused on the other side of the problem:

DA8 Russia avoids sanctions by operating covertly
DF1 A country's vulnerability is detected and targeted
DF2 Hybrid activities are detected and attributed.

Covert operations from a state actor targeting a country's vulnerabilities is an essential element of hybrid warfare, and in this context defined as 'hybrid operations': the second core uncertainty. Plotting these two core uncertainties as axes leads to the quadrant below, generating four possible scenarios. These scenarios will be developed in this chapter, with a focus on the threat a particular scenario would pose for the Netherlands. Although DF9 is a high-ranking driver, it is not taken into account in the core uncertainties, as its focus is on Russian criminal actors alone, and does not involve the Russian state in some way.


The plus side of the axes means that the scenario has a high or low level of that axis; so either there is a high/low level of cooperation between criminal actors and the Russian government, or there are many/few hybrid operations in Europe. This leads to four scenarios and end states:

**1. Home is where the heart is** *(high cooperation, low hybrid operations)*
End state: cooperation takes place, but in Russia, no or few hybrid operations in Europe

**2. Russian Hustle** *(high cooperation, high hybrid operations)*
End state: frequent hybrid operations in Europe, including a high involvement of criminal actors

**3. All Quiet on the Eastern Front** *(low cooperation, low hybrid operations)*
End state: government fights criminals, does not cooperate with them, and no hybrid operations

**4. The Professionals** *(low cooperation, high hybrid operations)*
End state: high level of hybrid operations in Europe, but by state actors; no cooperation with criminal actors taking place.

### 7.1 Home is where the heart is

*+ Cooperation - Hybrid operations*

In this scenario, the Netherlands is not directly targeted in Russian hybrid operations. This could be for a number of reasons, e.g. different Russian political goals that do not involve the Netherlands. Although it can be assumed that the Netherlands is a potential target for Russian hybrid operations, as is has been in the past, the country is probably not the highest priority in this domain. However, it is likely that the sanction regime plays a role in this as well: it has a large impact on the Russian economy which puts a heavy strain on the country, especially since COVID-19 and its economic consequences. By reducing hybrid operations in Europe, Russia can regain some of its goodwill with European countries.

Meanwhile, the Russian government and criminal actors in Russia increase their cooperation. This improves the government's grip on criminal actors and creates at the same time more possibilities for criminals that cooperate with the government: it gives them a certain level of protection from criminal prosecution, as long as they serve the state when requested. An increasing cooperation will therefore also hinder international criminal investigations, with the Russian state services being reluctant to provide data, evidence or extradite wanted criminals. Another consequence of this development, is the rise of corruption in Russian society and government, further transforming the country into a 'criminal-syndicalist state', where the legal world is deeply interconnected with the illegal world.[147] If this were to take place in Russia, there would be no direct threat to the Netherlands. However, if this development continues, Russia becomes an inherently unpredictable actor on the world stage, which could affect the Netherlands as well in the long run: there is high chance that illegal behaviour eventually will cross a country's borders.

**Indicators**

- Russian police reluctant to cooperate with international criminal investigations
- Top criminal leaders remain untouched by authorities
- Focus of Russian foreign policy on diplomatic relations and trade; improving relations with European countries
- Increasing corruption on all levels in the Russian government
- Increasing internal competition in the Russian criminal world
- Growing presence of Russian criminal actors in Europe

[147] CIS, "Organised Crime and the Special Services of the Commonwealth of Independent States," 2007.

### 7.2 Russian Hustle

*+ Cooperation + Hybrid operations*

This is without doubt the most dangerous scenario of all. In this scenario, an increasing cooperation between the Russian government and criminal actors is combined with an increase in hybrid operations across Europe. This results in a more embedded use of criminals in hybrid operations. In the past, criminal actors have been used by the Kremlin, but always indirectly embedded in the Russian operations. The closer connection between these two actors enables criminal actors to be directly embedded in hybrid operations.

Not only are criminals used by the Kremlin, but the Kremlin is also used by criminals. Hybrid operations are influenced by criminal interests: despite their cooperation with the state, criminal actors will continue pursuing their own interests. With the state as an ally, this will even be easier: the cooperation ensures limited pressure from internal or external police investigations, and limited access to the states' resources and capabilities, which dwarf those of criminal groups. These conditions would enable criminal actors to thrive, although it can also lead to more internal competition regarding who gets what. This would suit the Russian government, which has used the strategy of 'divide and conquer' before.

This scenario is dangerous for the Netherlands, as it has a serious impact on several important domains. First, Dutch foreign policy and the country's geopolitical position are put under pressure, as it needs to respond to Russian hostilities. Secondly, Dutch society is affected by both the hybrid operations aimed at it, and by a growing illegal economy, which undermines the legal economy.

**Indicators**

- Russian government reluctant to cooperate with international police investigations
- Increase in hybrid operations in Europe in the political, cyber or social domain
- Increasing internal competition in the Russian criminal world
- Growing presence of Russian criminal actors in Europe
- Hybrid operations carried out by government and criminal actors
- Denial of hybrid operations by Russian government
- Top criminal leaders remain untouched by authorities

### 7.3 All Quiet on the Eastern Front

*- Cooperation - Hybrid operations*

The third scenario is the least threatening option for the Netherlands. It entails a reduced or minimal cooperation between the state and criminal actors, and no hybrid operations aimed at the Netherlands. Though it is difficult to imagine such a peaceful scenario, it is important to imagine it, in order to prevent tunnel vision on escalating options.

As there is little or no cooperation between the Kremlin and criminal groups, crimefighting efforts are more efficient; both in and outside Russia. In Russia, investigations are opened, criminal leaders prosecuted and criminal organisations have trouble surviving. Corruption is fought more effectively throughout the government; it is increasingly difficult to buy power. The increasing internal pressure can cause criminal groups to emigrate, continuing their practices outside of Russia. However, international crime networks are dealt with transnationally; police services work together with their Russian counterparts in investigations that involve Russian citizens or assets. Given the effectiveness and resources of European police services, it is therefore likely that these criminal actors will prefer regions where there is with weaker government structures, giving them more freedom to act.

Furthermore, the foreign policy interests of Russia have shifted to such an extent that it is not actively waging hybrid operations aimed at the Netherlands. This can be for different reasons, as mentioned before, such as avoiding sanctions. In this scenario however, it has a stronger motivation. While regaining law and order internally, the Kremlin is also actively improving its geopolitical relations with Western countries. This can be from sheer desperation, given the weakening Russian economy and collapsing world economy, or from a more strategic viewpoint: China’s fast-growing economy can make Russia dependent on China within few years and it therefore needs strong partners to counter this development.

**Indicators**

- No active hybrid operations in Europe
- Stronger repression of crime in Russia
- Russia collaborates in international crime investigations
- Russia seeks to improve (economic) relations with the EU
- Spread of Russian criminal organisations in Europe

### 7.4 The Professionals

*- Cooperation + Hybrid operations*

The fourth scenario comes closest to the current situation. There is little cooperation between the Russian government and criminal actors on the strategic level, while Russian hybrid operations are targeting the Netherlands.

With this combination of factors, the status quo is maintained, mostly. Both actors stick to their area of expertise: criminal actors seek profit from illicit activities such as drug trafficking or laundering money. Intelligence and security services do what they do best (or so they assume): protecting the country's interest by any means necessary; in and outside of Russia. The Kremlin actively attempts to influence Western countries using hybrid tactics, while the absence of a strong response from the targeted countries only encourages the Kremlin to continue these operations. The behaviour of the intelligence agencies becomes only bolder, more visible; there seems to be little worry on being caught. Especially in the countries surrounding Russia, this behaviour is demonstrated: the Russian government acting as if nothing changed in 1991.

While Russian intelligence officers have free rain in Europe, criminals on the other hand, do not, especially not inside Russia. In the lower levels of government, criminal actors can gain some influence, but on the strategic level, they are kept on a very short leash. Criminal groups that become too powerful or embarrass the state in any way, are suppressed aggressively, even the powerful criminal leaders. Over the years, government doubles down on criminality; both on the street level and on higher levels. The only exception is when the state needs the particular skills of a group or individual: the occasional hacker or international arms dealer. This repression of criminality causes criminal groups to find their luck elsewhere, outside of Russia. Although they are still not completely safe from the Kremlin, European countries do provide a more welcoming environment for these groups.

**Indicators**

- Increase in Russian hybrid operations in the Netherlands
- Criminal actors are prosecuted in Russia
- Hybrid operations in Europe are solely carried out by personnel linked to Russian intelligence services
- Spread of Russian criminal organisations in Europe
- Denial of hybrid operations by Russian government

### 7.5 Implications

In this chapter, scenarios are developed based on the driver analysis in chapter 6, in order to get a perspective on possible future developments in this domain and thereby be able to better respond to this threat. From these scenarios and their corresponding indicators, several important lessons can be identified for the Netherlands, with regards to policymaking.

- First, it is important to keep track of the relationship of the Russian government and Russian criminal actors: whether the Kremlin uses criminal actors operations, and whether crimefighting efforts in Russia are effective. An increase or decrease in criminal investigations, especially into high-level criminal leaders, could indicate a change in this relationship.
- Second, the development of Russian criminal actor's presence in Europe should be closely monitored, especially the criminal groups that operate transnationally. The Netherlands has a small presence of Russian criminal actors, as indicated before, but international criminal groups could provide government services better access to the country.
- Third, although sanctions are often imposed after Russian hybrid operations, there is limited understanding of their effectiveness and to what extent they reach their intended purpose. More research into this aspect of hybrid warfare is therefore required.
- Fourth, international crimefighting is still the most effective method against criminal actors, in hybrid warfare and outside this context. Supporting and strengthening these efforts will thereby help to get a better grip on this complex problem.
- Finally, the threat of cybercrime increasingly looms over global society; it has the potential to have a far larger impact on people's lives than many other types of crime. It is therefore vital that the Netherlands ensures it is well-equipped to counter this type of threat in the coming years.

These lessons learned do not indicate an immediate threat for the Netherlands from criminal actors in Russian hybrid operations. However, there is a potential threat that should be closely monitored, as indicated above. In the following chapter, this is further developed and connected to the models introduced in chapter 4, in order to get a precise image of what this threat implies.

# 8 Conclusion

This study has sought an answer to the question 'How can Russia use criminal actors in the concept of hybrid warfare in the Netherlands?'. To find a conclusive answer to this question, a literature study was done to analyse the different concepts involved, which forms a basis for the second part of the thesis, in which scenarios are developed for the future development of this phenomenon.

*The Concept*
First, the concept of hybrid warfare was studied: how it developed, what the concept itself is, and what the Russian approach to hybrid warfare is. The concept is fairly new: it was introduced in 2015 and quickly gained popularity, describing modern warfare as a "merger of different modes and means".[148] Although the term is new, the practices of hybrid warfare are far from it: many elements of the concept appear in old, classical studies of war. When looking at hybrid warfare in the Russian context, several similarities can be found in the tactics of the Soviet Union, often labelled as 'subversion' and 'active measures'. Although there is an extensive conceptual debate on the Russian application of hybrid warfare, it often comes down to a core issue: a wide range of Russian activities that aims to influence and undermine countries' politics and institutions in undesirable ways, often aimed at Western countries.[149]

*The Actors*
Despite the amount of research that is done on this topic, there is little understanding of the relationships and role of actors in hybrid warfare. In an effort to get a better insight on this, this thesis zooms in on criminal actors and their role in hybrid warfare from three perspectives. First, the analysis focuses on the actors involved in the Russian concept of hybrid warfare. Second, the study looks at the possible relationships between actors in hybrid warfare, using a model with four different types of relationships on the axes of state/non-state and beneficiary/proxy. Third, a model for indicating an actor's function in hybrid warfare was applied to criminal actors, which helped to identify their function as largely as indirectly involved and either as a surrogate (a supporting role) or as a proxy (performing a task independently). These models are used to thoroughly analyse the subject of this study: criminal actors.

Through an extensive literature study on Russian criminal actors, a better understanding of their current capabilities and possibilities is developed. During the Soviet Union's transition to a market economy, both criminal and government actors seized this opportunity to gain economic and political power. This development is still visible: on different levels, the legal and the illegal economy are closely connected. Modern Russian-based criminals often operate globally, most as intermediaries for the underworld, and are increasingly sophisticated: there is a strong increase in more technical activities, such as cybercrime and economic crime. After a 'Russian crime-hype' in the 1990s, governments discovered that the influence of Russian criminal actors is rather limited. This was the case in the Netherlands as well: there are some Russian criminal actors active, but it is mostly seen as 'neutral' territory. Interestingly, the Russian-speaking community in the Netherlands has a different perspective on

[148] Mattis and Hoffman, "Future Warfare: The Rise of Hybrid Wars."
[149] Radin, Demus, and Marcinek, Understanding Russian Subversion.

the threat these actors pose: for them, the dangerous criminals are those infiltrating the economy, not the drug dealers. These financial crimes are at the same time difficult to get a grip on for police and investigative services.

*The Practice*
Criminal actors are often left out or barely present in hybrid actor-analyses, although there are multiple examples of their involvement in Russian operations. Russian criminal actors have been recruited by the Kremlin in several ways: in violent conflicts as mercenaries, to launch cyberattacks (either as the only method, or as part of larger operation) and in illegal arms trade. In other cases, a relationship is suspected but not proven, for example in assassinations, economic crimes and in their use as intermediaries. With these identified possibilities of the use of criminal actors, we can look at the next element of this thesis: the future development of this threat.

*The Perspective*
Building on this context, a SWOT analysis and a Causal Loop Diagram are used to identify the core uncertainties: the most important drivers in this context of the Netherlands. These two drivers (cooperation between criminal actors and the state / hybrid operations in Europe) form the basis of the scenarios, which help to develop a better perspective on how this threat can evolve in the future. Using the abovementioned methods (driver analysis and scenario building), this study has covered both the alpha and beta of this type of threat. The literature study and driver analysis covers the alpha: all the important options/threats. The scenario element covers the beta: reducing the chance to miss a possible development or relationship. Applying both elements in research into hybrid warfare has added value, as it widens the scope of the researcher and enriches the research by providing a broader view on a certain aspect of hybrid warfare.

*The Verdict*
The preceding paragraphs developed, by answering the sub-questions, the knowledge required to answer the research question: How can Russia use criminal actors in the concept of hybrid warfare in the Netherlands? This question will be answered in three steps. First, the conceptual framework and the case of the Netherlands are outlined. Next, a comprehensive view on the threat to the Netherlands is developed, answering this thesis' research question.

Focusing on the conceptual dimension of hybrid warfare, there are several possible relationships between actors in hybrid warfare. In the case of Russia, the two main relationships are the Russian state as beneficiary, and either state- or non-state actors as proxy. Identifying the different actors demonstrates the wide range of state and non-state actors the Russian government has at its disposal due to its strong control over, or influence on many institutions and groups. Although under exposed, criminal actors should be included in the category of non-state actors. Next, a model is used to specify the function of these actors which categorises criminal actors by their direct or indirect embeddedness; and by supplementary or delegatory morphology. In the case of criminal actors, this is an indirect relation, with either a delegatory or a supplementary role. This conceptual analysis thereby demonstrates the capability of the Russian government to use non-state actors for its political goals.

Looking at hybrid operations in the Netherlands, a historical precedent is visible. Hybrid operations have targeted Western countries since the period of the Soviet

Union, then called ‘subversion’ or ‘active measure’. The Netherlands is not an exception to this rule; numerous examples since the Cold War have been identified. Although it does not occur frequently, there are several recent cases that illustrate the continuing interest of the Russian government in the Netherlands to this day. This is not solely focused on the Netherlands as a country, but also on the country’s associations, such as the European Union and NATO. It can therefore be assumed that the use of non-state actors in this context applies to the Netherlands as well.

*Concepts & Scenarios*
Finally, when connecting the conceptual framework and the scenario building for the case of the Netherlands, the focus is on the type II relationship: the state as a beneficiary and the non-state actors as the proxy. Applying the models to the scenarios, there are a few interesting findings. First of all, all scenarios involve a type II-relationship, except for the third scenario, in which there is virtually no cooperation. The only relationship that would then be possible, is type III, where the state becomes the proxy of the non-state actor. Looking at the different functions of non-state actors, the possible functions in the first scenario are surrogate (indirect, supplementary) or proxy (indirect, delegatory); which corresponds with the analysis of the first part of the thesis. This largely applies to the second scenario as well, with one addition: in this scenario, a direct embeddedness would be possible; making criminal actors into auxiliary forces. Lastly, the fourth scenario only envisions criminal actors as surrogates, given the low level of cooperation with the state.

*Discussion*
Combining the lessons from the scenario building and the literature analysis, no direct threat of criminal actors being used to target the Netherlands is identified, but there is a potential threat. This can be for two different reasons: either the Netherlands is not a target of Russian operations, or different means are used for these operations, such as state actors. Because of this study’s focus on state/non-state relations, the state/state relations are not taken into account; this would require further research.

Applying the models used in this thesis helps in identifying and understanding criminal actors’ function in Russian hybrid warfare. However, at the same time there are limits to this classification. The function of criminal actors is fluid to such an extent that the usefulness of this classification can be questioned. This analysis does give a better grip on the phenomenon, but the changeable function of criminal actors should be taken into account in further research.

It is important to note the usability of the scenarios: they are not actual warning scenarios of a near or distant future, but aimed at policy-making. Therefore, the indicators to these scenarios are indicative indicators. In order to get a perspective on the actual threat criminal actors pose, a different method is necessary: it would require the development of warning scenarios and critical indicators, which would require more in-depth research into the specific categories of criminal activities and state involvement in these matters. The findings of this thesis vis-à-vis the threat for the Netherlands are therefore not ground-breaking in the absence of a direct threat, but the study’s approach is all the more interesting. By connecting history, creating a conceptual framework and an extensive case study of this phenomenon with regards to the Netherlands, this topic was studied thoroughly. Had the focus been on a specific type of crime, it could have led to interesting findings as well, but such a narrow approach has serious limitations. Because of the lack of evidence in many of

these cases, it would not have reached the same level of depth. Finally, although there is no direct threat for the Netherlands, there could be a threat for other countries, especially countries in conflict where Russia is involved. Studying this topic with a similar approach would therefore be all the more interesting in those cases.

# 9 Bibliography

Abramova, Irina. “The Funding of Traditional Organized Crime in Russia.” *Economic Affairs* 27, no. 1 (2007): 18–21. https://doi.org/10.1111/j.1468-0270.2007.00704.x.

Abrams, Steve. “Beyond Propaganda: Soviet Active Measures in Putin’s Russia.” *Connections: The Quarterly Journal* 15, no. 1 (2016): 5–31.

Al Jazeera. “Russian ‘Evil Corp’ Hackers Charged by US in $100m Cyber Theft ,” August 6, 2019. https://www.aljazeera.com/news/2019/12/russian-evil-corp-hackers-charged-100m-cyber-theft-191206054758063.html.

BBC News. “How the Dutch Foiled Russian ‘cyber-Attack’ on OPCW,” 2018. https://www.bbc.com/news/world-europe-45747472.

———. “Skripal Poisoning: Third Russian Suspect ‘Commanded Attack,’” 2019. https://www.bbc.com/news/uk-48801205.

———. “How Mexican Cartels Are Gaining from Covid-19 ,” July 10, 2020. https://www.bbc.com/news/av/world-latin-america-53343599/coronavirus-how-mexican-cartels-are-taking-advantage-of-pandemic.

Bellingcat. “Identifying The Berlin Bicycle Assassin: From Moscow to Berlin ,” December 3, 2019. https://www.bellingcat.com/news/uk-and-europe/2019/12/03/identifying-the-berlin-bicycle-assassin-part-1-from-moscow-to-berlin/.

Bellingcat Investigation Team. “The GRU Globetrotters: Mission London ,” June 28, 2019. https://www.bellingcat.com/news/uk-and-europe/2019/06/28/the-gru-globetrotters-mission-london/.

Bērziņš, Jānis. “Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy,” no. April (2014): 1–14.

Bettiza, Sofia. “Coronavirus: The Lure of Mafia Money during the Crisis .” BBC News , May 5, 2020. https://www.bbc.com/news/world-europe-52537573.

Blanton, Tom, and Svetlana Savranskaya. “NATO Expansion: What Gorbachev Heard.” National Security Archive, 2017. https://nsarchive.gwu.edu/briefing-book/russia-programs/2017-12-12/nato-expansion-what-gorbachev-heard-western-leaders-early.

Brown, Zachery Tyson. “Unmasking War’s Changing Character.” Modern War Institute, 2019. https://mwi.usma.edu/unmasking-wars-changing-character/.

Bunker, Robert J. “Unrestricted Warfare: Review Essay I.” *Small Wars & Insurgencies* 11, no. 1 (2000): 114–21. https://doi.org/10.1080/09592310008423265.

Caliskan, Murat. *Modern Political Warfare: Current Practices and Possible Responses*. *The RUSI Journal*. Vol. 164, 2019. https://doi.org/10.1080/03071847.2019.1621490.

Cheloukhine, Serguei. “The Roots of Russian Organized Crime: From Old-Fashioned Professionals to the Organized Criminal Groups of Today.” *Crime, Law and Social Change* 50, no. 4–5 (2008): 353–74. https://doi.org/10.1007/s10611-008-9117-5.

Chivvis, Christopher. “Understanding Russian ‘Hybrid Warfare’: And What Can Be Done About It.” 2017. https://doi.org/10.7249/ct468.1.

CIS. “Organised Crime and the Special Services of the Commonwealth of Independent States,” 2007.

CNN. “Inside the KGB,” 1998.

https://web.archive.org/web/20070627183623/http://www3.cnn.com/SPECIALS/cold.war/episodes/21/intervie ws/kalugin/.

Crezee, Bart. “Miljarden Dollars Aan Russisch Witwasgeld Belandden Op Nederlandse En Europese Rekeningen.” De Correspondent, 2017. https://decorrespondent.nl/6448/miljarden-dollars-aan-russisch-witwasgeld-belandden-op-nederlandse-en-europese-rekeningen-hoe-zit-dat-precies/1953713675056-2bee0fc5.

Department of Defense, United States of America. “Irregular Warfare (IW) Joint Operating Concept (JOC).” Vol. 1, 2007.

Der Spiegel International. “Trapping the Lord of War: The Rise and Fall of Viktor Bout ,” October 6, 2010. https://www.spiegel.de/international/world/trapping-the-lord-of-war-the-rise-and-fall-of-viktor-bout-a-721532.html.

Dewan, Angela, Milena Veselinovic, and Carol Jordan. “All the Countries Expelling Russian Diplomats.” *CNN*, March 28, 2018. https://edition.cnn.com/2018/03/26/europe/full-list-of-russian-diplomats-expelled-over-s-intl/index.html.

Dixon, Robyn. “Chechen Exiles Are Being Hunted down. Often, the Trail Leads Back to Russia.” *The Washington Post* , July 4, 2020. https://www.washingtonpost.com/world/europe/chechen-exiles-are-being-hunted-down-often-the-trail-leads-back-to-russia/2020/07/06/e16d9e12-bf68-11ea-864a-0dd31b9d6917_story.html.

Douven, Igor. “Abduction .” Stanford Encyclopedia of Philosophy, 2015. https://plato.stanford.edu/entries/abduction/#DedIndAbd.

———. “Peirce on Abduction .” Stanford Encyclopedia of Philosophy, 2015. https://plato.stanford.edu/entries/abduction/peirce.html.

Europol. “Two Main Russian Mafia Groups Dismantled in Spain with Europol’s Support,” August 28, 2017. https://www.europol.europa.eu/newsroom/news/two-main-russian-mafia-groups-dismantled-in-spain-europol’s-support.

Finckenauer, James O., and Elin J. Waring. *Russian Mafia in America: Immigration, Culture, and Crime*. Boston: Northeastern University Press, 1998.

Finckenauer, James O. “The Russian ‘Mafia.’” *Society Abroad*, 2004, 61–64.

Finckenauer, James, and Yuri Voronin. “The Threat of Russian Organized Crime.” *Issues in International Crime*, 2001.

Foreign Affairs Committee. “Moscow’s Gold: Russian Corruption in the UK,” 2018.

Galeotti, Mark. “Crimintern: How the Kremlin Uses Russia’s Criminal Networks in Europe.” *The Oxford Handbook of Organized Crime*, no. January (2014): 1–12.

———. “Hybrid, Ambiguous, and Non-Linear? How New Is Russia’s ‘New Way of War’?” *Small Wars & Insurgencies* 27, no. 2 (2016): 282–301. https://doi.org/10.1080/09592318.2015.1129170.

———. “‘Hybrid War’ and ‘Little Green Men’: How It Works, and How It Doesn’t,” n.d.

———. “I’m Sorry for Creating the ‘Gerasimov Doctrine.’” Foreign Policy, 2018. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.

———. “The Russian ‘Mafiya’: Consolidation and Globalisation.” *Global Crime* 6, no. 1 (2004): 54–69. https://doi.org/10.1080/1744057042000297972.

———. “The Vory.” Yale University Press Podcast, 2018. https://www.stitcher.com/podcast/yale-university-press-podcast/e/55006781.

Galeotti, Mark, and Radio Free Europe. “Crime And Crimea: Criminals As Allies

And Agents." Radio Free Europe, n.d. https://www.rferl.org/a/crimea-crime-criminals-as-agents-allies/26671923.html.

Gerasimov, Valeriy. "Науки В Предвидении." *Military Industrial Courier* 8, no. 476 (2013): 2–3. https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf.

Giegerich, Bastian. "Hybrid Warfare and the Changing Character of Conflict." *Connections: The Quarterly Journal* 15, no. 2 (2016): 65–72. https://doi.org/10.11610/Connections.15.2.05.

Giles, Keir. "Russia's 'New'' Tools for Confronting the West.'" *Russia and Eurasia*. Vol. 1, 2016. https://doi.org/10.1515/sirius-2017-0037.

Goldman, Marshall I. "Putin and the Oligarchs." Council on Foreign Relations, 2004. https://www.cfr.org/world/putin-oligarchs/p8018.

Grabo, Cynthia M. "Anticipating Surprise: Analysis for Strategic Warning." Joint Military Intelligence College, 2012.

Gray, Colin S. *Fighting Talk : Forty Maxims on War, Peace, and Strategy*. Praeger Security International, 2007.

———. *War, Peace and International Relations: An Introduction to Strategic History*. 2nd ed. New York: Routledge, 2012.

Guriev, Sergei, and Andrei Rachinsky. "The Role of Oligarchs in Russian Capitalism." *Journal of Economic Perspectives* 19, no. 1 (2005): 131–50. https://doi.org/10.1257/0895330053147994.

Halper, Stefan. "China: The Three Warfares," 2013, 1–566.

Hammarberg, Thomas. "Human Rights in Areas Affected by the South Ossetia Conflict." *Commissioner for Human Rights*, 2008.

Harding, Luke, Caelainn Barr, and Dina Nagapetyants. "Everything You Need to Know about the Azerbaijani Laundromat." The Guardian, 2017. https://www.theguardian.com/world/2017/sep/04/everything-you-need-to-know-about-the-azerbaijani-laundromat.

Havlik, Peter. "EU-Russia Sanctions Exchange Has Had Important Economic and Political Consequences," February 20, 2019. https://wiiw.ac.at/n-365.html.

Hoffman, Frank G. "On Not-so New Warfare: Political Warfare vs. Hybrid Threats." War on the Rocks, 2014. https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.

Hoffman, Frank G. "Conflict in the 21st Century:," n.d., 72.

———. "Conflict in the 21st Century: The Rise of Hybrid Wars." Arlington, VA: Potomac Institute for Policy Studies, 2007.

———. "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges." *Prism* 7, no. 4 (2012): 31–47.

Johnson, Robert. "Hybrid War and Its Countermeasures: A Critique of the Literature." *Small Wars & Insurgencies* 29, no. 1 (2018): 141–63. https://doi.org/10.1080/09592318.2018.1404770.

Kaldor, Mary. *New and Old Wars : Organized Violence in a Global Era*. Cambridge: Polity Press, 2013.

Kapusta, Philip. "The Gray Zone," 2015.

Kilinskas, Kęstutis. "Hybrid Warfare: An Orientating or Misleading Concept in Analysing Russia's Military Actions in Ukraine?" *Lithuanian Annual Strategic Review* 14, no. 1 (2016): 139–58. https://doi.org/10.1515/lasr-2016-0006.

Kuijpers, Karlijn. "Nederlandse Banken Zijn Een Schakel in Russische Miljardenfraude ." *De Groene Amsterdammer*, March 3, 2019. https://www.groene.nl/artikel/nederlandse-banken-zijn-een-schakel-in-russische-miljardenfraude.

Landmeter, Erik De. "The Relevance of Clausewitz's 'On War' to Today's Conflicts."

*De Militaire Spectator*, 2018. https://www.militairespectator.nl/thema/strategie/artikel/relevance-clausewitzs-war-todays-conflicts.

Lind, William S., Keith Nightengale, John F. Schmitt, Joseph W. Sutton, and Gary I. Wilson. “The Changing Face of War: Into the Fourth Generation.” Marine Corps Gazette, 1989. https://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html.

Macrotrends. “Russia Crime Rate & Statistics 1990-2020,” 2020. https://www.macrotrends.net/countries/RUS/russia/crime-rate-statistics.

Mälksoo, Maria. “Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO.” *European Security* 27, no. 3 (2018): 374–92. https://doi.org/10.1080/09662839.2018.1497984.

Mattis, James N, and Frank G Hoffman. “Future Warfare: The Rise of Hybrid Wars.” *U.S. Naval Institute Proceedings* 131, no. 11 (2005): 18–19.

Maurer, Tim. “Cyber Proxies on the Loose: The Former Soviet Union.” *Cyber Mercenaries*, 2017, 94–106. https://doi.org/10.1017/9781316422724.007.

———. “Proxies: An Instrument of Power Since Ancient Times.” In *Cyber Mercenaries*, 21:29–49. Cambridge: Cambridge University Press, 2017. https://doi.org/10.1017/9781316422724.003.

Merriam Webster. “Deduction,” 2020. http://www.merriam-webster.com/dictionary/deduction.

Merriam Webster. “Deductive vs. Inductive vs. Abductive Reasoning,” 2020. https://www.merriam-webster.com/words-at-play/deduction-vs-induction-vs-abduction.

Merriam Webster. “Induction,” 2020. http://www.merriam-webster.com/dictionary/induction.

NATO. “A Short History of NATO.” NATO Declassified. Accessed May 7, 2020. https://www.nato.int/cps/en/natohq/declassified_139339.htm.

NCTV. “Χίμαιρα, Een Duiding van Het Fenomeen ‘Hybride Dreiging,’” 2019, 1–36. https://www.nctv.nl/documenten/rapporten/2019/04/18/duiding-fenomeen-hybride-dreiging.

NISA. Spionagecentrum in Tsjechoslowaakse ambassade, Ingelicht § (2002).

Noordaa, Robert Van der, and Coen Van der Ven. “Nepnieuws Uit Sint-Petersburg.” *De Groene Amsterdammer*, 2019.

Normark, Magnus. “How States Use Non-State Actors : A Modus Operandi for Covert State Subversion and Malign Networks,” 2019, 1–8.

OCCRP. “The Russian Laundromat Exposed ,” March 20, 2017. https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/.

OCCRP. “The Proxy Platform,” 2011. https://www.reportingproject.net/proxy/en/the-proxy-platform.

Olink, Hans. “Sebald Rutgers (1879-1961), Nederlands Ingenieur in de Sovjet-Unie.” *Historisch Nieuwsblad*, no. 1 (2014). https://www.historischnieuwsblad.nl/sebald-rutgers-1879-1961-nederlands-ingenieur-in-de-sovjet-unie/.

Radin, Andrew, Alyssa Demus, and Krystyna Marcinek. *Understanding Russian Subversion: Patterns, Threats, and Responses*. RAND Corporation, 2020. https://www.rand.org/pubs/perspectives/PE331.html.

Rauta, Vladimir. “Towards a Typology of Non-State Actors in ‘Hybrid Warfare’: Proxy, Auxiliary, Surrogate and Affiliated Forces.” *Cambridge Review of International Affairs*, 2019, 1–20. https://doi.org/10.1080/09557571.2019.1656600.

Reichborn-Kjennerud, Erik, and Patrick Cullen. “What Is Hybrid Warfare?” *NUPI Policy Brief* 1 (2016). http://brage.bibsys.no/xmlui/bitstream/handle/11250/2380867/3/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf.

Renz, Bettina. “Russia and ‘Hybrid Warfare.’” *Contemporary Politics* 22, no. 3 (2016): 283–300. https://doi.org/10.1080/13569775.2016.1201316.

Ricks, Thomas, and Oscar Jonsson. “How Russia Stumbled into a Winning Strategy to Undermine the West.” *Foreign Policy*, March 29, 2017. https://foreignpolicy.com/2017/03/29/how-russia-stumbled-into-a-winning-strategy-to-undermine-the-west/.

Rojansky, Matthew, and Michael Kofman. “A Closer Look at Russia’s ‘Hybrid War.’” *Kennan Cable*, 2015. https://www.wilsoncenter.org/publication/kennan-cable-no7-closer-look-russias-hybrid-war.

Rosner, Lydia S. “The Sexy Russian Mafia.” Accessed June 16, 2020. http://orgcrime.tripod.com/russexy.htm.

Saric, Ivana. “Europol Helps Break Up Two Smuggling and Trafficking Gangs.” OCCRP, June 18, 2019. https://www.occrp.org/en/daily/9987-europol-helps-break-up-two-smuggling-and-trafficking-gangs.

Schwartz, Mathew J. “Why Russian Cybercrime Markets Are Thriving ,” July 28, 2010. https://www.bankinfosecurity.com/russian-cybercrime-markets-are-thriving-a-8439.

Shelley, Louise I. “Post-Soviet Organized Crime: Problem and Response.” *European Journal on Criminal Policy and Research* 3–4 (1995).

Siegel, Dina. “Russian Biznes in The Netherlands,” 2002.

South China Morning Post. “Russia’s Feared Mafia Leaders in ‘Shock’ as Vladimir Putin Shows Who’s Boss ,” March 8, 2019. https://www.scmp.com/news/world/russia-central-asia/article/3001483/russias-feared-mafia-leaders-shock-vladimir-putin.

Stubbs, Jack, and Christopher Bing. “Hacking the Hackers: Russian Group Hijacked Iranian Spying Operation, Officials Say.” *Reuters UK*, October 21, 2019. https://uk.reuters.com/article/uk-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUKKBN1X00AX.

Thomas, Timothy. “The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking.” *Journal of Slavic Military Studies* 29, no. 4 (2016): 554–75. https://doi.org/10.1080/13518046.2016.1232541.

Thornton, Rod. “The Changing Nature of Modern Warfare: Responding to Russian Information Warfare.” *The RUSI Journal* 160, no. 4 (2015): 40–48. https://doi.org/10.1080/03071847.2015.1079047.

Thucydides. “The History of the Peloponnesian War.” Accessed April 23, 2020. https://history.hanover.edu/courses/excerpts/211thuc.html.

Tzu, Sun. *The Art of War*. Edited by Lionel Giles. London: Sterling Publishers Pvt.Ltd, 1994. http://www.gutenberg.org/files/132/132-h/132-h.htm.

“U.S. Sanctions on Russia,” January 17, 2020. https://fas.org/sgp/crs/row/R45415.pdf.

US Department of Justice. “Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of ‘Bugat’ Malware ,” December 1, 2019. https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens.

Valk, Giliam G. de. “Dutch Intelligence - towards a Qualitative Framework for Analysis.” University of Groningen, 2005.

Varese, Federico. *The Russian Mafia: Private Protection in a New Market Economy*. Oxford: Oxford University Press, 2001.

———. “The Structure and the Content of Criminal Connections: The Russian Mafia in Italy.” *European Sociological Review* 29, no. 5 (2013): 899–909. https://doi.org/10.1093/esr/jcs067.

Volkov, Vadim. “Who Is Strong When the State Is Weak: Violent Entrepreneurs in Post-Communist Russia.” *Russia at the End of the Twentieth Century*, 1998, 1–32.

Waterval, Dirk. “Tienduizenden Witwasmeldingen, Amper Strafzaken. ‘Soms Lijkt Het of Het Hele Meldsysteem Voor Niets Is.’” *Trouw*, July 27, 2020. https://www.trouw.nl/economie/tienduizenden-witwasmeldingen-amper-strafzaken-soms-lijkt-het-of-het-hele-meldsysteem-voor-niets-is~b03c7f64/.

Weenink, Anton. “General Crime Pattern Analysis Eastern Europe.” *The Cambridge Handbook of Forensic Psychology*, no. October (2002): 159–65. https://doi.org/10.1017/cbo9780511730290.020.

———. “The Russian Mafia: A Private Actor in International Relations?” In *Non-State Actors in International Relations*, 55. Farnham: Ashgate Publishing Limited, 2001.

Weenink, Anton, and Franca van der Laan. “The Search for the Russian Mafia: Central and Eastern European Criminals in the Netherlands, 1989-2005.” *Trends in Organized Crime* 10, no. 4 (2007): 57–76. https://doi.org/10.1007/s12117-007-9012-y.

Weissmann, Mikael. “Hybrid Warfare and Hybrid Threats Today and Tomorrow: Towards an Analytical Framework.” *Journal on Baltic Security* 5, no. 1 (2019): 17–26. https://doi.org/10.2478/jobs-2019-0002.

Wolfowitz, Paul. “Intelligence Policy-Relations.” *Policy*, 1994, 35–42.

Zaitch, Damian. “Bosses, Brokers and Helpers.” In *The Extremes of Social Space: Ways of Thinking About Changes at the Top and the Bottom of Advanced Transatlantic Societies*, 502–29. Amsterdam, 2002.

# 10 Appendix

1. Paired ranking drivers