NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(SAS-161)TP/1173

www.sto.nato.int

STO TECHNICAL REPORT **TR-SAS-161-Vol-II**

The NATO STO SAS-161 Research Task Group (RTG) – Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices

Volume II: Information and Influence

(Le groupe de recherche (RTG) SAS-161 de la STO de l'OTAN – Aspects militaires de la lutte contre la guerre hybride : expériences, enseignements, meilleures pratiques.

Volume II : information et influence)

This volume of SAS-161 presents case studies from Canada, Denmark (focused on Kosovo), Sweden, and Ukraine. All investigate various aspects of Russian information and influence activities.

Published February 2024

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(SAS-161)TP/1173

www.sto.nato.int

STO TECHNICAL REPORT **TR-SAS-161-Vol-II**

The NATO STO SAS-161 Research Task Group (RTG) – Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices

Volume II: Information and Influence

(Le groupe de recherche (RTG) SAS-161 de la STO de l'OTAN – Aspects militaires de la lutte contre la guerre hybride : expériences, enseignements, meilleures pratiques.

Volume II : information et influence)

This volume of SAS-161 presents case studies from Canada, Denmark (focused on Kosovo), Sweden, and Ukraine. All investigate various aspects of Russian information and influence activities.

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published February 2024

ISBN 978-92-837-2485-8

Table of Contents

List of Figures

Acknowledgements

The SAS-161 RTG could not have conducted its work, particularly through the challenges of the pandemic and then, for our Ukrainian members, in the face of the existential threat created by Russia's full invasion of their country, without the support of many people. The NATO Liaison Office Kyiv facilitated the initial translation of Volume I from Ukrainian to English. The NATO STO Collaboration Support Office (CSO) in Paris, the staff at the Political Affairs & Security Policy Division in Brussels, the NSHQ J9 Staff in Mons, staff at Defence Research and Development Canada, Centre for Operational Research and Analysis (DRDC CORA) in Ottawa, and the staff of the Croatian Defence Academy "Dr. Franjo Tuđman", in Zagreb all provided the support required for the RTG to conduct our meetings and workshops. The Zagreb Security Forum (ZSF), led by RTG member Dr. Gordan Akrap, created the opportunity to present preliminary results at the October 2022 ZSF. The ZSF is truly a superb platform for forthright discussion of important and sensitive topics. Ukraine has proven, once again, to be an ideal scientific collaborator and we thank the National Defence University of Ukraine and the NATO-Ukraine Platform for Countering Hybrid Threats for sponsoring this collaboration and assisting in the travel of our Ukrainian members.

SAS-161 Membership List

CO-CHAIRS

Mr. Neil CHUKA*
Defence Research and Development Canada CORA
CANADA
Email: NEIL.CHUKA@forces.gc.ca

Col Dr. Viacheslav SEMENENKO**
National Defence University of Ukraine
UKRAINE
Email: semenenko17viacheslav@gmail.com

MEMBERS

Assist. Prof. Gordan AKRAP
Hybrid Warfare Research Institute
CROATIA
Email: gakrap@yahoo.de

Ms. Dorthe BACH NYEMANN*
Royal Danish Defence College
DENMARK
Email: dony@fak.dk

Dr. Jānis BĒRZIŅŠ
National Defense Academy of Latvia
LATVIA
Email: janis.berzins01@mil.lv

Dr. Jan BREN
Centre for Security and Military Strategic Studies
CZECHIA
Email: jan.bren@unob.cz

Dr. Byron HARPER
Allied Special Operations Forces Command
Deputy, J9 Partnership Division
Email: byron.harper@nshq.nato.int

Ms. Linda JARL*
Swedish Defence Research Agency (FOI)
SWEDEN
Email: linda.jarl@foi.se

Mr. Matthew LAUDER*
DRDC
CANADA
Email: Matthew.Lauder2@ecn.forces.gc.ca

Col. Janne MÄKITALO
Finnish Army Academy
FINLAND
Email: janne.m.makitalo@mil.fi

Cpt. (ret.) Ivica MANDIĆ
St. George Association
CROATIA
Email: vcmndc@gmail.com

Mr. Giles READER
Dstl
UNITED KINGDOM
Email: greader@dstl.gov.uk

Ms. Jeanette SERRITZLEV*
Royal Danish Defence College
DENMARK
Email: jese@fak.dk

*** Contributing or supporting author of Volume II, Information and Influence**

**** Ukraine Project Lead**

ADDITIONAL CONTRIBUTORS

Volodymyr BASHYNSKYI*
State Scientific Research Institute of Armament and Military Equipment Testing and Certification
UKRAINE
Email: dndivs@ukr.net

Mr. Petr MATOUS
Czech Ministry of Defence
CZECHIA

Hennadii PIEVTSOV*
Ivan Kozhedub Kharkiv National Air Force University in Science
UKRAINE
Email: pgvn@ukr.net

Pavlo OPEN'KO*
National Defence University of Ukraine
UKRAINE
Email: pavel.openko@ukr.net

Anatolii SALII*
National Defence University of Ukraine
UKRAINE
Email: saliy-a@i.ua

PANEL/GROUP MENTOR

Mr. Sean BOURDON
Defence Research and Development Canada CORA
CANADA
Email: sean.bourdon@forces.gc.ca

*** Contributing or supporting author of Volume II, Information and Influence.**

The NATO STO SAS-161 Research Task Group (RTG) – Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices

Volume II: Information and Influence

(STO-TR-SAS-161-Vol-II)

Executive Summary

The NATO STO SAS-161 Research Task Group (RTG) investigating "Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices" is meant to inform the full spectrum of military planning at the Alliance and national level. This functionally oriented analysis touches all aspects of military effectiveness and help inform our collective efforts to account for the challenges of contemporary, and expected future characteristics, of competition, conflict, warfare, and warfighting.

With a focus on contributing to the long-term military effectiveness of the Alliance, Ukraine, and the individual Ally and Partner nations, the RTG applied the fundamentals of net assessment in developing two distinct research streams. Both research streams study contemporary Russian behaviors related to competition, conflict, warfare, and warfighting. The first stream further investigates, from Ukraine's perspective, Russian aggression against Ukraine and Ukrainian institutional responses and preparations up to the full-scale invasion by Russia on 24 February 2022. The second research stream, undertaken by the non-Ukrainian members of the RTG, develops national or mission-specific case studies investigating Russian behaviors within differing contexts. The intent of this second stream is to identify military-specific aspects of those behaviors. The analysis and deductions related to each research stream are then combined and distilled into military implications.

The case studies in this volume demonstrate the importance of close study of Russian, or any threat actor's, behaviors, in a manner cognizant of the specific context of that actor. In other words, seeking to identify generic threat characteristics is less useful for planning purposes than understanding each threat on its own, at least in the first instance. The examination of KFOR and Canadian deployments to Latvia and Ukraine expose some erroneous assumptions of likely Russian behavior and targets. This conclusion is shared by several of the case studies presented in Volume III of the SAS-161 reporting. Jarl's and Lauder's case studies suggest some divergent conclusions. Whereas Jarl's case study illustrated centralization of control and interconnected, complementary military, political, and informational dimensions for Russian strategic level messaging related to large military exercises, Lauder's case study exposes decentralized execution and more simplistic means of execution. The characteristics noted by Lauder can be seen in the description of Russian activity in other case studies as well, notably Reader's and Bērziņš' chapters in Volume III. Much like the Finnish case study presented in Volume IV of our reporting, the Ukrainian case study here illustrates the high value of evidence and expertise required for the development of plausible scenarios. For both near and long-term military planning, a net assessment approach demands that any scenarios developed are grounded in as much evidence as possible to ensure plausibility. This is the case even when the intent is to push the bounds into low likelihood, high impact types of events. This rule holds true regardless of the scenario purpose – exercise or experimentation, forecasting, foresight, or near-term planning. Finally, the scenario development described in the case study employs updated Ukrainian legal, policy, and doctrinal frameworks to set the context of the development process and analysis of the scenarios. This contributes to the proven high accuracy reflected in later real-world events. This example thereby reinforces the importance of comprehensive national level security and defence arrangements – a conclusion mirrored in the case studies in Volumes III and IV of our reporting.

Le groupe de recherche (RTG) SAS-161 de la STO de l'OTAN – Aspects militaires de la lutte contre la guerre hybride : expériences, enseignements, meilleures pratiques

Volume II : Information et influence

(STO-TR-SAS-161-Vol-II)

Synthèse

Le groupe de recherche (RTG) SAS-161 de la STO de l'OTAN – « Aspects militaires de la lutte contre la guerre hybride : expériences, enseignements, meilleures pratiques » vise à éclairer tout le spectre de la planification militaire au niveau de l'Alliance et au niveau national. Cette analyse fonctionnelle aborde tous les aspects de l'efficacité militaire et éclaire nos efforts collectifs visant à tenir compte des caractéristiques actuelles et futures (prévues) de la concurrence, des conflits, de la guerre et des combats.

En se concentrant sur la contribution à l'efficacité militaire à long terme de l'Alliance, de l'Ukraine et des pays alliés et partenaires, le RTG a appliqué les principes fondamentaux de l'évaluation nette pour établir deux axes de recherche distincts. Les deux axes de recherche étudient les actuels comportements russes liés à la concurrence, aux conflits, à la guerre et aux combats. Le premier axe étudie plus en détail, du point de vue de l'Ukraine, l'agression de la Russie contre l'Ukraine et les préparatifs et réponses institutionnelles de l'Ukraine jusqu'à l'invasion à grande échelle par la Russie le 24 février 2022. Le deuxième axe, suivi par les membres non ukrainiens du RTG, développe des études de cas nationales ou propres à une mission, qui examinent les comportements russes dans différents contextes. L'objectif de ce deuxième axe est d'identifier les aspects spécifiquement militaires de ces comportements. L'analyse et les déductions liées à chaque axe de recherche sont ensuite combinées et aboutissent à des implications militaires.

Les études de cas du présent volume démontrent combien il est important d'examiner minutieusement les comportements russes, ou de tout acteur menaçant, en ayant conscience du contexte particulier de l'acteur en question. En d'autres termes, il est moins utile de chercher à identifier les caractéristiques générales des menaces à des fins de planification que de comprendre chaque menace, du moins dans un premier temps. L'examen du déploiement de la KFOR et des forces canadiennes en Lettonie et en Ukraine met en évidence le caractère erroné de certaines hypothèses relatives au comportement et aux cibles probables de la Russie. Plusieurs études de cas présentées dans le volume III des rapports du SAS-161 partagent cette conclusion. Les études de cas de Jarl et de Lauder suggèrent quelques conclusions divergentes. Tandis que l'étude de cas de Jarl illustre la centralisation du contrôle et des dimensions (complémentaires et interconnectées) militaires, politiques et informationnelles pour les messages stratégiques russes liés aux grands exercices militaires, l'étude de cas de Lauder présente l'exécution décentralisée et des moyens d'exécution plus simples. Les caractéristiques notées par Lauder apparaissent également dans d'autres études de cas décrivant l'activité russe, notamment les chapitres de Reader et Bērziņš dans le volume III. Tout comme l'étude de cas finlandaise présentée dans le volume IV de nos rapports, l'étude de cas ukrainienne illustre ici la grande valeur des preuves et l'expertise requise pour élaborer des scénarios plausibles. Pour la planification militaire à court et long terme, la démarche de l'évaluation nette exige que tous les scénarios développés s'appuient sur autant de preuves que possible afin de garantir la plausibilité. Cela vaut même lorsque l'intention est de repousser les limites jusqu'aux types d'événements à faible probabilité et à fortes répercussions.

Cette règle s'applique quel que soit l'objectif du scénario : exercice ou expérimentation, prévision, étude prospective ou planification à court terme. Enfin, l'élaboration du scénario décrit dans l'étude de cas emploie des cadres juridiques, politiques et doctrinaux ukrainiens mis à jour, qui définissent le contexte du processus d'élaboration et de l'analyse des scénarios. Cela contribue à une grande précision, éprouvée par les événements ultérieurs du monde réel. Cet exemple souligne ainsi l'importance d'accords nationaux complets en matière de sécurité et de défense, conclusion reflétée dans les études de cas des volumes III et IV de nos rapports.

Chapter 1 – INTRODUCTION

Neil CHUKA
Defence Research and Development
CANADA

The NATO STO SAS-161 Research Task Group (RTG) investigating "Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices" is meant to inform the full spectrum of military planning at the Alliance and national level. The functionally oriented analysis and the country-specific case studies developed by the RTG touch all aspects of military effectiveness and help inform our collective efforts to account for the challenges of contemporary, and expected future characteristics, of competition, conflict, warfare, and warfighting.

Defence scientific research and development activities must, in the first instance, seek to contribute to the military effectiveness of the forces they support. Military effectiveness is defined as:

> *the proficiency with which armed forces convert resources into fighting power. A fully effective military is one that generates maximum combat power from the resources physically and politically available to it. The most important attribute of military effectiveness is the ability to adapt to the actual conditions of combat and conflict (vice those that were assumed would occur). Military effectiveness is comparative and can only be assessed against a likely opponent or a rigorous composite adversary through a pacing threats construct.*[1]

Military effectiveness has political, military-strategic, operational, and tactical level components and is inextricably tied to military learning, adaptation, and innovation.[2] As might be expected, military effectiveness is defined differently depending on the purpose of the individual scholar. While we ascribe to Williamson Murray and Alan Millett's national and organizationally-focused construct, others have focused on the ability of military formations to generate, apply, and reconstitute combat power [6]. Still others apply notions of effectiveness at what we might call the service or environmental level (e.g., Army, Navy, Airforce, etc.) [7], [8]. Scholars have also applied Murray and Millett's framework to assess gaps in tactical level military effectiveness as a means of correcting national level political, social, and military historiography [9]. Of greater, more recent frequency, many have built upon Murray and Millett and their individual and combined work investigating learning, adaptation, and military innovation to focus on the specifics of the intersection of technology, doctrine, organizational culture, and other factors, and the implications for military effectiveness in contemporary times [10], [11], [12], [13], [14], [15]. Regardless of the particular focus, all of these consider political (inclusive of socio-cultural, economic, and other national factors), military-strategic, operational, and tactical issues affecting the ability of the armed forces to achieve desired ends.

Notions of military effectiveness color the work of many scholars in several fields of study, even if the words "military effectiveness" are not explicitly used. Moreover, the use of the words "military effectiveness" by authors certainly predates the work of Murray and Millett but their framework has proven sufficiently resilient to stand the test of time and, even if used as a foil, the phrase has been employed in multiple academic fields of study.[3] It is for this reason that we loosely apply the military effectiveness framework as a guide for the work of SAS-161. The framework is relatable to a substantial body of serious academic and professional literature, it provides an innate flexibility that enables the integration of a broad range of

[1] The military effectiveness definitions employed here originate in Millett et al. [1] pp. 1-27. These were adapted specifically for force development and design purposes by Chuka [2] and Chuka and Neill [3].

[2] See for example the essays in Murray and Millett [4] and Murray [5].

[3] On predating, see for example Sutherland [16].

subjects and helps focus our analysis for a particular purpose – the provision of STO support to the NATO military instrument of power.

1.1 BACKGROUND

The SAS-161 RTG is the second Systems and Analysis Studies (SAS) activity conducted in collaboration with Ukraine. During the period 2015 – 2017, the SAS-121 Research Specialist Team (RST) investigated in detail the Russian annexation of Crimea and the instigation of its campaign in Eastern Ukraine.[4] That collaborative research activity demonstrated the earnest, forthright desire of our Ukrainian partners to investigate Russian methods of conflict, warfare, and warfighting, share their experiences, and work closely with NATO. The intent of SAS-121 was to contribute to the study and learning of contemporary conflict and warfare to help collective efforts to address shared security and defence challenges.

SAS-161 follows in the path of SAS-121 by studying the military aspects of countering hybrid warfare to better understand individual and collective experiences, develop and share lessons, and identify best practice. This present work partnered the National Defence University of Ukraine (NDUU) with analysts from Canada, Croatia, Czechia, Denmark, Finland, Great Britain, Latvia, and Sweden, and NATO SOF HQ (NSHQ) via the SAS Panel and the STO Collaboration Support Office (CSO). The work was Co-Chaired by Canada and the NDUU. At the NDUU, the "Project Kalmius" team was led by the Ukrainian Co-Chair of SAS-161, Colonel Viacheslav Semenenko.

Our work has two distinct research streams, both focused on studying Russian behaviors related to competition, conflict, warfare, and warfighting. The first stream further investigates, from Ukraine's perspective, Russian aggression against Ukraine and Ukrainian institutional responses and preparations *up to* the full-scale invasion by Russia in February 2022. The second research stream was undertaken by the non-Ukrainian members of the RTG and sees the development of national or mission-specific case studies investigating Russian behaviors in specific differing contexts. The intent of this second stream is to identify military-specific aspects and implications of that behavior.

1.2 METHOD

Designed and approved in October 2019, the SAS-161 work program seeks to provide a unique contribution to the broader literature on "hybrid" or contemporary warfare by best exploiting the talents of, and the information available to, the RTG members, all of whom are involved in defence planning or professional military education systems at the national or Alliance level. In an effort to differentiate from some other portions of the very large, and growing, body of literature on hybrid warfare, the RTG work program was designed to adhere to the fundamentals of "net assessment" while striving to produce analysis focused on the aforementioned conception of military effectiveness.

Net assessment is the comparative analysis of military, technological, political, economic, and other factors governing the relative military capability of nations.[5] Its purpose is to identify problems and opportunities that deserve the attention of senior defence officials [19], p.9. Net assessment is a practice that applies distinctive perspectives to identify problems, including organizational and socio-bureaucratic behavior within specific contexts, as a means of determining meaningful balance of force estimates and plausible strategic interactions to inform decision making (adapted from Ref. [20]). A Net Assessment mindset works to strengthen critical thinking while countering received wisdom or group think and is most valuable where it fosters the provision of contested advice to decision-makers. Most importantly, a net assessment mindset demands the study of ourselves and our adversaries both.

[4] The final report of that RST is entitled "Research Specialist Team on Hybrid Warfare: Ukraine Case Study" [17].

[5] The following three paragraphs are adapted from Chuka and Archambault [18], pp.7-8.

For military planning purposes, net assessment is focused on power relationships: it is a means of capturing and orienting decision-makers to the exploration of strategic interactions – in all their complexity and variables – between and among actors in the operating environment as a way to expose gaps and opportunities. This allows analysts to better understand contexts and what constitutes relevant change in the strategic environment that affects military decision making.[6] As analysts, it also allows us, in fact forces us, to characterize the bounds of competitive military space. In support of an estimative process, net assessment frames military problems as strategic interactions as a way to think about choices and their impacts [23]. And it forces us to contain our analysis within the boundaries or parameters of a particular time period.

In this way, net assessment is an approach – a way of thinking – that incorporates all-source and inter-disciplinary material and recognizes the intellectual necessity of both nurturing and managing contested advice at an organizational level. Net assessment, therefore, is not only, potentially, a "capacity" or a "capability" as it has been recently described in various restricted distribution Alliance documentation.[7] As such, it is not surprising that organizations deal with it hesitantly, certain that it might be necessary, but uncertain as to how or why. For instance, the 2010 NATO Strategic Concept calls on the Alliance to ensure it is "at the front edge in assessing the security impact of emerging technologies, and that military planning takes the potential threats into account." Such admonition calls out for comparative assessment in aid of pursuing the strategic objective of maintaining competitive advantage over potential adversaries – but of course does not explicitly refer to "net assessment" [24], p.17. Neither, then, is it surprising that net assessment is variously considered to be a product, a capability, a process, an intellectual construct and a methodology. Nonetheless, both analysts and practitioners should embrace net assessment as an organizational mindset or approach that works to strengthen critical thinking while countering received wisdom or "group think," rather than pursue it as an "authoritative" singular endeavor or point of departure for planning.[8]

With this in mind, the SAS-161 work program is guided by relatively straightforward parameters comprised of three pillars.

The first pillar is the focus on the *military* aspects of contemporary competition, conflict, warfare, and warfighting. While political, economic, financial, and other factors are relevant to some of the individual studies comprising the SAS-161 body of work, those non-military factors are only considered insofar as required to understand their military implications within the context of a particular case study. This focus does not disregard the interplay between the military and other instruments of power; rather, we apply this focus to help identify gaps in military authorities, responsibilities, legal frameworks, and policy that are exposed during the research and analysis. This is critical as the SAS-161 work is conducted under the auspices of the Alliance's Science and Technology Organization (STO) and therefore must contribute to the use, development of, and effectiveness of the military instrument of power.

The second pillar is that Russia, inclusive of proxies and others that might contribute to Russian goals, is the sole threat actor under consideration. While other threat actors might apply methods similar to those of Russia, adherence to the principles of net assessment means that each threat actor (and target – e.g., Ukraine or any of the states considered in our case studies) must be considered in their own context. Broadening the

[6] See Gouré [21], pp. 90-97. Gouré explains the relationship between net assessment and the development of competitive strategies, recognizing that there are several acceptable definitions and usages of "net assessment." For an excellent discussion of the origins of net assessment and the role of Dr Andrew Marshall in its development and implementation see Adamsky [22], pp. 611-644.

[7] There is very little Alliance documentation on this point that can be referenced in an unclassified publication. The author has participated in unclassified Alliance meetings where this point has been made by others.

[8] This should not be interpreted as a claim that comparative assessment does not occur naturally – as Cohen has observed, the appraisal of military balances "goes on all the time in the minds of decision-makers and their staffs" [25], p. 4. The argument we are making here is the importance of improving upon stale threat-agnostic capability based planning methods.

research and analysis to include other threat actors risks studying the methods rather than the actor – something that is arguably of limited utility for military planning purposes and, regardless, has been done by many others.[9]

The third and final pillar is the preference for contemporary primary source material in the research and analysis. As much as possible given the intent to work at the unclassified level, the members of the RTG employ original official documentation, interviews, and other similar material considered to be primary source. This requirement is meant to emphasize and exploit the specialized knowledge and perspective held by the RTG members and thereby distinguish it from analysis conducted by those outside of defence institutions.

No single project can be comprehensive and SAS-161 is no exception to this rule. For example, there is limited detailed discussion of the use of space or cyber capabilities and the case studies are not intended to span all recent targets of Russian malevolence or those countries that fall within Russia's self-proclaimed sphere of interest. Nonetheless, our research and analysis contribute to the broader body of work on contemporary competition, conflict, and warfare and contribute to the effort to better understand ourselves and Russia as an adversary.

With these parameters, the case studies and the Ukrainian Project Kalmius research and analysis were developed independently under central direction and guidance from the Co-Chairs. This approach maximized the disparate professional and educational backgrounds and perspectives of the RTG members.

The implications development process described in the "Military Implications" volume of our reporting was then used to distil the military implications from the collated main analytic deductions identified in each individual piece of work. Military implications are defined as:

> *The implied consequences of credible deductions arrived at through the application of professional judgment. An implication should be actionable, without identifying courses of action, and relate to one or more capability components or enablers in order to inform military planning. For operational research and analysis, any implication is likely to affect multiple functional areas, can identify new requirements, validate current capability paths, or suggest capabilities of declining relevance. Implications must centre upon military effectiveness and credibility*. (Adapted from Ref. [28]).

The implications development process allows for the identification of commonalities and contrasts across all of the main deductions, enabling the integration of the entire body of RTG scholarship into a whole.[10] The incorporation of an implications development process as a core portion of the work program reinforces our focus on the military aspects of hybrid approaches and the application of such methods by a specific threat actor (Russia). The result is a specific set of recommendations tailored to planning functions. Consequently, we remain within the scope and intent of the NATO STO SAS mandate, respectful of the role and authorities of those executing planning functions in NATO and national level headquarters and remain true to the framework of academic and professional literature on military effectiveness and net assessment that provided the intellectual guidance in the development of the RTG work program.

[9] See for example, Giannopoulos et al. [26]. A public version of this document was produced in 2012. See also the Multinational Capability Development Campaign Countering Hybrid Warfare project and series of publications. A summary of that work is available at: MCDC CHW project [27].

[10] A similar process assessed the results of the SAS-121 analysis from a NATO perspective. That work is captured in the SAS-127 final report entitled "Hybrid Warfare: Implications for NATO" [29].

1.3 OVERVIEW OF ANALYSIS

The specific topics covered in this volume of SAS-161 reporting are detailed in the next section. Overall, however, there are some major deductions resulting from the work as a whole.

Ukraine provides an exemplar of military effectiveness grounded upon superb military adaptation and flexibility. The current effectiveness of Ukraine's armed forces is rooted in almost 9 years of work that has modernized and transformed Ukraine's conceptions of security and defence with the support of a wide variety of international partners. As with any situation, there is an historical and contemporary context that must be appreciated and accounted for but all those interested in security and defence affairs will do well to study Ukraine's actions to glean insight and lessons.

The reporting confirms the imperative to study each threat in a way that respects the context of adversary decision making and the specifics of behaviors directed at each target. Conversely, each target of Russian malevolence must be studied to understand the historic and contemporary conditions that create both vulnerabilities and shields against the Russian threat. Even when faced with multiple threats it is important that each is understood individually before designing comprehensive responses. In other words, a net assessment mindset applied to threat-based planning will result in greater understanding of threat, strengths, vulnerabilities, and risk.

Our analysis helps to highlight that, at the national level, the concept of "total defence" or "comprehensive defence" (e.g., the idea that national security and defence must be seen as a whole-of-government and whole-of-civil society responsibility) is the foundation of military effectiveness, at least from a homeland defence perspective. This is because such conceptions of national defence help clarify the role of military forces in relation to other instruments of national power and, hopefully, contribute to high levels of military political effectiveness.[11]

Finally, despite the fact that much of the work of the SAS-161 RTG was conducted remotely, in a distributed fashion, first because of the pandemic and latterly because of the full-scale Russian invasion of Ukraine, collaborative projects such as this contribute to our ability to reach greater levels of understanding and improve our knowledge on contemporary security and defence challenges.

1.4 TOPICS COVERED IN THIS VOLUME

This volume of reporting from SAS-161 presents case studies focused on information and influence by examining Russian, Alliance, and partner activities in a variety of contexts. Using an analytic framework of "Frontstage / Backstage" Linda Jarl analyzes Russian strategic military exercises, and Russia's reaction to a NATO Trident Juncture exercise, to improve understanding of Russian use of military and non-military effects. Dorthe Bach Nyemann and Jeanette Serritzlev discuss Russian influence activities in, and on, Kosovo, with the objective being to uncover Russian information activities targeting KFOR and the overall Alliance presence in the area. As with the analysis by Mr. Giles Reader in Volume III of our reporting, the KFOR case study suggest that Russia has been very careful, and limited, in directly targeting Alliance formations or deployed elements. Our partners from the National Defence University of Ukraine contribute a discussion explaining the development and use of threat-based scenarios focused on the informational aspects of Russian behavior for the purposes of forecasting in planning activities. In doing so they

[11] Military Political Effectiveness is defined as: The effort to obtain resources for military activity in relation to the goals set by the polity and the proficiency in acquiring those resources. Resources consist of reliable access to financial support, a sufficient military-industrial base (including assured access), a sufficient quantity and quality of manpower, and control over conversion of those resources into military capabilities. Military political effectiveness hinges on a clear understanding of national grand strategy. This necessarily includes strong comprehension of vital national interests, the enduring and immediate threats to those interests, and a grasp of likely activities and tasks and the resources to carry out those activities and tasks to counter the threats to those interests.

demonstrate, by virtue of the relative accuracy of events that came to pass after the chapter was drafted, the importance of solidly grounding foresight and forecasting activities with evidence and expertise. This volume is closed out by Matt Lauder's case study of the operational context, mechanics, and impact of Russian information confrontation targeting Canadian deployments to Latvia and Ukraine. In doing so, the case study illustrates the importance of understanding that much of Russia's approach to information confrontation is focused on applying consistent pressure to promote Russian narratives and undermine those of the Alliance and Alliance members. Moreover, and similar to several of the case studies in the SAS-161 analysis, much of Russian information confrontation is indirect, rather than explicit. Annex A contains a table linking the military implications in Volume V of the SAS-161 reporting to the case studies. The abbreviations CAN, DNK (KFOR), SWE, UKR denote the case studies in this volume.

1.5 REFERENCES

[1] Millett, A., Murray, W., and Watman, K. "The Effectiveness of Military Organizations." In A. Millett and W. Murray (eds.), Military Effectiveness: Volume 1 The First World War. New Edition, NY: Cambridge University Press, 1988/2010, pp. 1-27.

[2] Chuka, C. "Learning From (Recent) History? An Assessment of CF Joint-Level Learning, Innovation, and Adaptation Activities." DRDC CORA TM2013-048, Ottawa: DRDC, March 2012.

[3] Chuka, N. and Neill, D. "A Research and Analysis Framework for a Strategic-Level Lessons Learned Process." DRDC CORA TM 2011-210. Ottawa: DRDC, December 2011.

[4] Murray W., and Millett, A. (eds.), Military Innovation in the Interwar Period. NY: Cambridge University Press, 1996/2007.

[5] Murray, W. Military Adaptation in War. Alexandria VA: Institute for Defense Analysis, 2009.

[6] Mansoor, P. The GI Offensive in Europe: The Triumph of American Infantry Divisions, 1941 – 1945. Lawrence: Kansas: University Press of Kansas, 1999.

[7] Reese, R. Why Stalin's Soldiers Fought: The Red Army's Military Effectiveness in World War II, Lawrence, Kansas: University Press of Kentucky, 2011.

[8] Hill, A. The Red Army and the Second World War. Cambridge UK: Cambridge University Press, 2020.

[9] Harward, G. Romania's Holy War: Soldiers, Motivation, and the Holocaust. Ithaca: Cornell University Press, 2021.

[10] Marcus, R. Israel's Long War with Hezbollah: Military Innovation and Adaptation Under Fire. Washington DC: Georgetown University Press, 2018.

[11] Finkel, M. On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield. Stanford CA: Stanford University Press, 2011.

[12] Mansoor, P., and Murray, W. (eds.), The Culture of Military Organizations. Cambridge: Cambridge University Press, 2019.

[13] Jungdahl, A. and Macdonald, J. "Innovation Inhibitors in War: Overcoming Obstacles in the Pursuit of Military Effectiveness." Journal of Strategic Studies, 38(4), 2015, pp 467-499.

[14] DeVore, M. “Armaments After Autonomy: Military Adaptation and the Drive for Domestic Defence Industries.” Journal of Strategic Studies, 44(3), 2022, pp. 325-359.

[15] Tomes, T. Military Innovation and the Origins of the American Revolution in Military Affairs. Unpublished doctoral dissertation, University of Maryland, 2004.

[16] Sutherland, R.J. “Organization for Military Effectiveness.” ORD Informal Paper No. 66/P10, Ottawa: Department of National Defence Operational Research Division, May 1966.

[17] NATO STO, “Research Specialist Team on Hybrid Warfare: Ukraine Case Study.” STO-TR-SAS-121, Neuilly-sur-Seine, France: NATO Science and Technology Organization, February 2018.

[18] Chuka, N. and Archambault, P. “Improving Joint Force Development and Design: Applying Concept-Based, Threat-Informed Principles to NATO Capability Development.” DRDC-RDDC-2022-L052, Ottawa: DRDC, March 2022.

[19] US DoD, DoD Directive 5111.11, “Director of Net Assessment.” 14 April 2020.

[20] Bracken, P. “Net Assessment: A Practical Guide” Parameters, Spring 2006.

[21] Gouré, D. “Overview of the Competitive Strategies Initiative.” in T.G. Mahnken (ed.), Competitive Strategies for the 21st Century: Theory, History and Practice, Stanford: Stanford University Press, 2012, pp. 90-97.

[22] Adamsky, D. “The Art of Net Assessment and Uncovering Foreign Military Innovations: Lessons From Andrew W. Marshall’s Legacy.” Journal of Strategic Studies, 43(5), 2020, pp. 611-644.

[23] Skypek, T. “Evaluating Military Balances Through the Lens of Net Assessment: History and Application.” Journal of Military and Strategic Studies, 12(2), Winter 2010, pp. 6-9.

[24] Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. NATO: Brussels, November 2010.

[25] Cohen, E. Net Assessment: An American Approach. Tel Aviv: Jaffee Center for Strategic Studies, April 1990.

[26] Giannopoulos, G., Smith, H., and Theocharidou, M. The Landscape of Hybrid Threats: A Conceptual Model (Public Version). European Commission, Ispra, 2020.

[27] Multinational Development Capability Campaign Countering Hybrid Warfare (MDCC CHW) Project. Countering Hybrid Warfare postcard (publishing.service.gov.uk) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/783087/MCDC_Countering_Hybrid_Warfare_Postcard-web.pdf (Accessed April 2023).

[28] Chuka, N., Archambault, P., Auger, A., Gladman, B., Robinson, E., Taylor, B., and Wallace, B. “Implications Development Framework.” DRDC-RDDC-2018-L167, Ottawa: DRDC, July 2018.

[29] NATO STO. “Hybrid Warfare: Implications for NATO.” STO-TR-SAS-127. Neuilly-sur-Seine, France: NATO Science and Technology Organization, May 2018.

Chapter 2 – ANALYSIS OF RUSSIAN MILITARY EXERCISES

Linda Jarl
Swedish Defence Research Agency (FOI)
SWEDEN

2.1 INTRODUCTION[1]

The security situation in Europe is tense and more unpredictable due to the Russian annexation of Crimea and Georgian regions[2] as well as the war against Ukraine. Russia's strategies in Europe are demonstrated through a wide range of both non-military and military actions. According to Herta, several analysts and researchers highlight important changes in Russian strategies such as cyber and information warfare [1] p. 58; [2], [3]. while other scholars focus on the asymmetric nature of Russia's operations [1] p. 58. Nevertheless, the general term "hybrid warfare" has been used to explain Russia's strategies in Eastern Ukraine over the last ten years [1] p. 53.

Russia's practice of hybrid warfare has been analyzed in two previous NATO studies, "STO-TR-SAS-121 Research Specialist Team on Hybrid Warfare: Ukraine Case Study" [4] and "STO-TR-SAS-127 Hybrid Warfare: Implications for NATO" [5]. These studies highlighted that Russia increased its troop numbers and equipment at the same time they arranged military exercises near the Ukrainian border in March 2014. Consequently, the exercises functioned as an excuse to build up troops near Ukraine. In some cases, it was believed that the purpose of these actions was to create a deterrent effect and demonstrate resolve or a pre-phase to intervention. Exercises together with intelligence actions, surveillance, and reconnaissance activities were organized and complemented each other [4].

Military strategic exercises in Western Europe are increasing, as are Russian exercises [6]. The NATO-associated exercises "Trident Juncture" and the Russian "Zapad exercise" are both reoccurring and expanded military arrangements in the Baltic Sea area. Unfortunately, military exercises and military activities in the Baltic Sea area sometimes lead to tensions between Russia and Western states.[3] However, research concerning military exercises is sparse, especially in the context of hybrid warfare.

As part of the project "NATO SAS-RTG-161 – Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices," this case study seeks to enhance knowledge of Russian military exercises and how they might be used as an instrument with both military and non-military effects. The case study will examine and exemplify Russian behavior during strategic military exercises in the Baltic Sea area. This environment is interesting since it is geographically near Russia and a part of Russia's zone of operations. Another reason is that the Baltic Sea area works as a venue, or a "scene of meetings", between Russia on one side, and the neighboring states, the NATO-alliance and US on the other side. On background on the previous problematization, two questions are central to this case study:

- What kind of military and non-military actions does Russia use related to their strategic exercises in the Baltic Sea area?
- How does Russia respond by military or/and non-military means when NATO holds a strategic exercise near the Baltic Sea area?

[1] The author greatly appreciates the assistance of the research coordinator and the security political analyst at the Swedish Defence Research Agency (FOI) who peer reviewed earlier versions of this case study, providing valuable insights and suggested improvements. In addition, the author extends thanks to the head of department for operations and management at FOI.

[2] Regions of Abkhazia and Tskhinvali region/South Ossetia.

[3] Andorra; Australia; Austria; Belgium; Canada; Croatia; Czechia; Denmark; Estonia; Finland; France; Germany; Great Britain; Hungary; Iceland; Ireland; Italy; Latvia; Lichtenstein; Lithuania; Luxembourg; Monaco; Netherlands; New Zealand; Norway; Poland; Portugal; Slovakia; Slovenia; Spain; Sweden; Switzerland; and the Vatican.

Methodologically, the case study is based on a qualitative text analysis involving research articles, public documents, political statements and media articles. In order to enhance the understanding of how Russia may use military exercises, the empirical part of the case study focuses on Russian behavior during some of the most extensive strategic exercises in the Baltic Sea area, Zapad 2017 and Zapad 2021, as well as counter actions during the NATO strategic exercise Trident Juncture-18. It could be noted that Russia also arrange a considerable number of smaller exercises in the Baltic Sea area that might be of interest, however, they are not the scope of this chapter due to the focus on strategic exercises and the potential messages they address to a wide audience such as NATO and US. The empirical data is analyzed through the lens of an analytical concept grounded in theories of frontstage and backstage acting, introduced in Section 2-3.

The study is based on unclassified information. For natural reasons, access to data involving Russian military exercises as well as NATO's exercises is limited. As part of testing plans and military capability, there is a tendency within states to not reveal all information about the training process and potential weaknesses within. Consequently, it is important to keep in mind that full disclosure of details in military exercises is not possible or expected. However, the case study will shed light on potential gaps between what is communicated about military exercises and when they are conducted. The next chapter will present an overview of previous research.

2.2 THE MULTIFACETED NATURE OF MILITARY EXERCISES

Previous studies on the topic of military exercises have focused on analysis of military capability [7], the way operations are organized (e.g., Petraitis [8]), effects of escalation [9] as well as exercises in the context of political communication [1], types of military exercises [10] and information warfare [11].

Military forces are among the most important tools within a State, even though is it uncertain how they might be used and what signals they send to other parties. Military exercises, moreover, take place somewhere between peace and war, as a way of increasing the military capability and a preparation for a potential war [6], p. 15. Despite the end of the Cold War and decades of peace, the importance of military training in world politics is shown in the increasing trend of multinational military exercises. This includes both traditional military exercises used for deterrence or war rehearsals as well as non-traditional military exercises used to build relationship between states [10], p. 27.

A number of scholars have highlighted the multidimensional nature of military exercises, meaning that it is a form of collective training with a wide range of purposes. In addition to training the military capability of a nation's troops, military exercises involve fostering alliance unity and defence diplomacy. Exercises also contain a variety of outcomes and effects outside of training [12], p. 20. It has been argued that military exercises may escalate conflicts, but this seems to depend on the settings of the training. During the Russian strategic exercise Zapad 2017, some analysts claimed that Russia pushed the exercises to Belarus as a statement. It was believed that Russia's intention was to affect Belarus not to follow Georgia's and Ukraine's efforts to bond military and economically with NATO and Western states [9] p. 11, [13].

In their study, Kuo and Blankenship found that in Joint Military Exercises (JMEs), alliances offer institutional frames and establishment of strategic limitations for allies. Consequently, potential conflict escalation effects of exercises were dampened by the alliances joint organization [9] p. 1. The authors argued that alliances and JMEs form complementary parts of a "relational contract" [9] p. 9, which meant a type of long-term exchange between parties. Accordingly, JMEs accompanied with allies decrease the probability of conflict escalation [9] p. 9.

In another study, Heuser and Simpson found that multinational coalition and state-building exercises often contain both a military and a political dimension, but that the latter is often lacking in construction and performance. Without considering the political dimension, the consequences of the exercises, for the nations involved as well as neighboring countries, could not be foreseen and may lead to further tensions [12], p. 21.

Russian strategic exercises are considered by foreign viewers and neighboring states to have an intimidating effect. In some cases, there have been concerns that Russia might use military exercises as a pretext to mask preparations for potential and actual invasions. During the joint Russian and Belarusian strategic exercise Zapad 2021, for example, European and US observers expressed concern about aggression in the direction of allies in the region [14]. A study based on a discourse analysis of Zapad 2017 showed that information operations were part of the war game and that fear was constructed in the Russian strategic narrative [11] pp. 21-22.

The military exercise Ground Pepper held by NATO in 2014 is an example of how strategic intentions can be turned into military activities with a variety of purposes and audiences. Public messages sent by NATO included that the exercise Ground Pepper should test readiness to respond to military and non-military threats, which could be compared to the security situation in Europe at the time. The exercise was a way of reassuring and supporting eastern European members threatened by the security situation. However, this reassurance to Allies was, at the same time, a message of deterrence for the Russian Government not to hinder NATO countries [12] p. 22.

Exercises may reveal limitations and weaknesses to adversaries, and there may also be a period of increasing tensions and misunderstanding between parties during the exercise period [12] pp. 24-25, [15] p. 439. In order to reduce the risk of conflict and increase transparency, exercises with more than 9,000 participants should be announced to OSCE in accordance with the Vienna Document 2011 [16]. Identification of gaps within the agreement initiated a political discussion about the need of an update of the document [17]. It has been suggested that the intent of exercises involving 5,000 participants or more should be communicated to the OSCE, which would mean lowering the current limit of 9,000 participants. However, in 2016, Russia refused to update the agreement with OSCE regarding communicating the size and format of exercises [12] p.25. Due to the war in Ukraine, the update of the Vienna Document 2011 has been a subordinated question between states.

The next chapter presents a theoretical framework that will help to analyze Russian actions connected to military exercises. The theory offers a multifaceted perspective on human behavior, interactions and intentions.

2.3 THEORY OF FRONTSTAGE AND BACKSTAGE ACTING

Originally established by the sociologist Erving Goffman, the theory of frontstage and backstage has been further developed in later studies. One of these is Ruth Wodak's discourse analysis of political processes [18]. Goffman's theories are relevant because of the possibility to understand human behavior in different situations and how interactions are affected by social norms and rules. One might say that Goffman lay focus on social interactions and rules of individuals while Wodak extends this to include political processes. Wodak follows the reality of politicians "behind the scenes" as well as the public life of politicians and the decision making processes. Another aspect that she follows is how images of politicians are constructed on television.

The theory of frontstage acting is characterized by public behavior, visible elements of performance, and actors being on stage "doing something" or performing an act in front of an audience. According to Goffman, the term 'performance' refers to all the activity of an individual, which occurs during a period marked by the person's presence in front of a set of observers. Specifically, frontstage is where the performance takes place and the performers and the audience are present. It also means that the performer has some influence on the observers [19] p. 13. To give an example, when a representative of the Russian Ministry of Defence (MoD) makes a speech about military exercises to the media, this spokesperson acts frontstage. The information might interest a wide audience.

There are three important components of the front: appearance, setting and behavior. Appearance relates to how the performer looks, setting means the scenery or the location in which the performer is acting, and

behavior relates to what the performer does [18] p. 8. The setting involves the décor, physical lay-out and other background items, which supply the stage and scenery [19] p. 13. An example related to this case study might be a naval officer who, expected to fulfill his or her tasks during a military exercise, needs access to a scene and décor such as fleet, equipment, and personnel. Goffman also uses the term personal front, which can be understood as referring to characteristics of an individual such as rank, clothing, whether it is a woman or a man, looks and speech patterns [19] p. 14.

In contrast, backstage is where "performers are present but the audience is not, and the performers can step out of the character without fear of disrupting the performance" [18] p. 10. Information and informal actions that appear backstage are closed to the audience, who are not allowed to enter the backstage [18] p. 10. The access to backstage is controlled and limited by gatekeepers, which can be exemplified by a reception to a department, in which employees need a certain identification in order to enter the office. When performers are backstage, they are engaged in another sort of acting which is related to the members of a particular community [18] pp. 10-11. For instance, a political leader who has informal meetings with his or her colleagues.

Belief, dramatic realization and mystification are also relevant in Goffman's theory. Belief means that a person must believe in the part he or she is playing in order to perform, even though, it might be difficult for others to understand if it is real or an act [18] p. 8, [19]. Dramatic realization refers to what the performer wants the audience to know as well as how the performer speaks and acts to convince others. This may involve persuasive strategies in speeches or acting that seem to follow expectations from the audience and acting in a trustworthy way [18] p. 8. Wodak explains that the performer "has to make sure that he or she sends out the correct signals and quells the occasional compulsion towards misleading ones that might distract from the performance. Employing misleading rhetorical signals would confuse the audience and potentially destroy trust" [18] p. 8.

Mystification represents secrets and the concealment of specific information from others (the audience). Secrets are important characteristics in every organization and indicate power relations [18], [19] p. 17. The concealment of information is exclusively for the invited, the insiders who might share the secrets. In this way, mystification creates a social distance between those who are invited and those who are excluded. Hints of the information may lead to greater interest and curiosity among those who do not have access to the hidden information [18] p. 9.

2.3.1 Analytical Concept

In order to analyze a sample of military exercises in depth, I will present an analytical concept that is based on the theory of frontstage and backstage, and complemented by theoretical tools from the field of discourse analysis. Previous research shows that military exercises are multifaceted, with different meanings and effects. It is possible to identify at least a military and political dimension. Additionally, military exercises have an informational dimension in that they may create communicative value when sending political signals. For this reason, the analytical concept includes three dimensions: political, informational and military. Figure 2-1 visualizes the theoretical framework that will be used in the case study of Russian military exercises.

First of all, Figure 2-1 illustrates the notion of military exercises, and second of all how this activity is performed through frontstage and backstage acting. In this context, frontstage acting specifically refers to Russian public behavior when they are "on the scene" in front of a potential audience. For example, Russia could decide to act visible in the military dimension when conducting a military exercise or to what degree they seek to display a military parade to external audiences.

In addition, Russia is considered to act openly in the military dimension when conducting exercises. Russia also performs in the information domain when, for example, the Russian MoD speaks or produces public texts about the military exercises (i.e., military discourse). The political dimension consists of political performances and relations to other politicians, political (and economic) boundaries between states, relations

and political agreements/contracts that affect exercises. As mentioned before, the Vienna Document 2011 is an example of a key document, in which a significant number of states have agreed to follow certain rules and expectations in order to ensure transparency and trust.

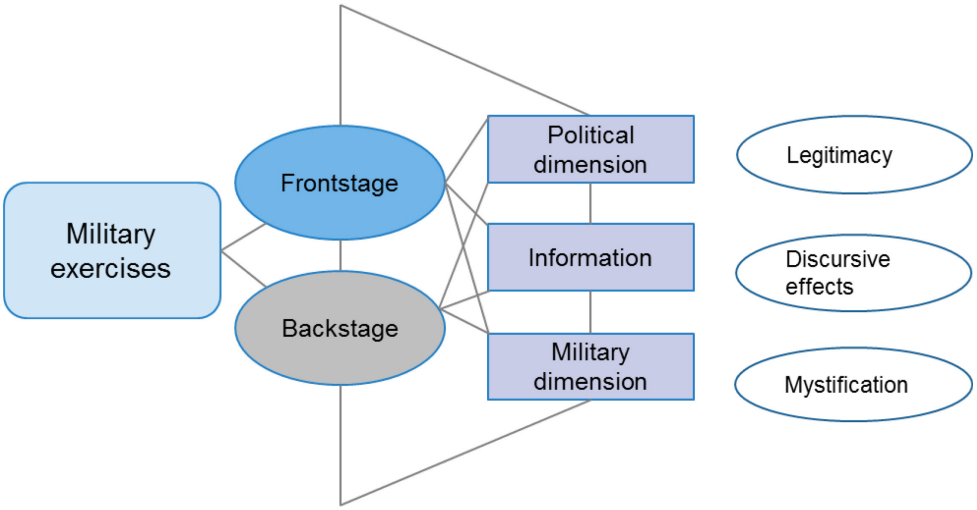

Figure 2-1: Theoretical Framework for the Study of Russian Military Exercises.

Backstage refers to Russian behavior behind the scenes that is characterized by non-transparency, internal matters, inclusion-exclusion, privacy, back door solutions and hidden decision processes. For example, when Russia decides to hide some stages of military exercises they are considered to be part of backstage acting in the military dimension. Another example of backstage acting, connected to both the informational and potentially the political dimension, are secret meetings in which unofficial information and intelligence is shared and/or decisions are made.

The notion of *legitimacy* has roots in discursive institutionalism, a direction within constructivism that follows the process from the appearance of suggestions, to their distribution, and finally to acceptance [20] p. 895. In other words, it refers to the procedure through which an idea becomes an accepted decision by others. In this study, legitimacy refers to the measures and strategies that Russia uses in the political and informational dimensions in order to construct legality.

The production of speeches, text and films about Russian exercises forms terminologies and a frame of a military discourse. The language and the way that messages are produced serve different purposes. *Discursive effects* defines how knowledge and power within a discourse are produced and exerted [21].

Mystification denotes information that is only accessible by an exclusive group or organization and is for the most part concealed to others. Access to information and knowledge may offer a position of power and a social distance to others. Indications of the hidden information may lead to greater awareness and interest among excluded parties [18] p. 9.

2.4 RUSSIAN MILITARY AND NON-MILITARY ACTIONS

This chapter aims to identify the kinds of military and non-military actions that Russia is using in the Baltic Sea area/northern Europe. The first section provides an introduction to Russian military exercises and is followed by two examples of Russia's established strategic exercises that reoccur every four years: Zapad 2017 and Zapad 2021. The final part of the chapter demonstrates how Russia responds by military or/and non-military means when NATO holds a major strategic exercise near the Baltic Sea area.

2.4.1 Russian Military Exercises

Annual strategic command staff exercises and combat readiness inspections are two types of military exercises conducted by the Russian military as part of its training. The exercises test Russia's military readiness, evaluate new equipment and technologies, improve operational concepts and develop command and control [14]. The military training year is organized in a winter training period from December to April and a summer training period from June to October [22]. Each Military District (MD) arranges a Strategic Command Staff Level Exercise once every four years and, since 2016, covers the following directions:

- Kavkaz 2016 in Southern MD;
- Zapad 2017 in Western MD;
- Vostok 2018 in Eastern MD;
- Tsentr 2019 in Central MD;
- Kavkaz 2020 in Southern MD; and
- Zapad 2021 in Western MD.

Additionally, the Russian MoD has reorganized the MDs and raised the Northern Fleet to a MD. This means that the number of MDs has increased from four to five [14]. This formalization and upgrading also reflects a renewed focus in the northern direction.

During the period 2009 to 2017, Russian military exercises increased in number and their character changed. Norberg points out that the most interesting thing is not the fact that they increased, but *how* the exercises changed. For instance, he noticed that Russia was able to run parallel exercises at different locations at the same time and that the transport capability was an important part in several arrangements. There was a higher degree of resources involved and the training organization grew [7].

In addition, Russia takes part in multinational exercises in Eurasia as a member of the intergovernmental military alliance, Collective Security Treaty Organization (CSTO). The other participants in CSTO are Belarus, Armenia, Kazakhstan, Kyrgyzstan and Tajikistan. There is also a cooperation between CSTO and the Shanghai Cooperation Organization (SCO) that includes China [23]. On a number of occasions, CSTO members have been invited to join strategic exercises in the Baltic Sea, such as when Kazakhstan recently joined Zapad 2021. Both Russia and Belarus took part in the Zapad exercises 2017 and 2021 [24], which also reflects the relationship and cooperation between the nations.

As this study is limited to exercises in the Baltic Sea area, only the Zapad exercises and an example of Russian behavior during one NATO exercise will be discussed further.

2.4.2 The Zapad Exercises

The Zapad exercises have a long history and can be traced back to the Cold War and the Soviet Union era, in which several exercises included propaganda against the West. The Zapad exercises have shown growing anti-Western attitudes [11] p. 24. In some cases, Russia has not updated or officially reported information about Zapad before it was held. For example, the number of participants and amount of resources involved in Zapad 2013 was greater than proclaimed. Around 13,000 troops were expected to join the exercise in 2013 but afterwards the actual number of participants was 25,000 (in other words, near double) [8], p. 238.

Since Russia's illegal annexation of Crimea, states in the West and NATO have highlighted the increasing number of military exercises. In their study, Aronsson and Ottosson point to the increasing number of training arrangements by NATO or NATO members. A greater number of participants from several countries joined the exercises that were characterized by a geographical spread, more complexity and

training of advanced capabilities.[4] Budgets for exercises have increased and the number of exercises has also increased in Northern and Eastern Europe [5], p. 10, p. 21. This also means that NATO's engagement is visible near the Russian sphere of influence.

2.4.3 Zapad 2017

Zapad 2017 was a joint military exercise between Belarusian and Russian Armed Forces, arranged in the Belarus and in the regions of Kaliningrad, Leningrad and Pskov. The exercise was held between 14 – 20 September and was labeled a defensive anti-terror exercise [25]. The Russian MoD declared that 12,700 troops, around 680 pieces of military hardware, up to 70 aircraft and 10 warships were involved in the exercise [26]. Zapad 2017 had multiple goals, including training of military troops, testing new weapons and synchronization of accomplishments [11] p. 22, [27].

According to information from the MoD, the exercise was based on a scenario in which terrorist groups gain access to the Russian and Belarusian territories with the aim of destabilizing the Union State of Belarus and Russia. In the scenario, the terrorists are provided with logistics and military resources from external parties [25].

The European security context in which Zapad 2017 was held, included tensions between Russia and NATO and the West in general. The armed conflict in Ukraine was still ongoing. During this time, Russia was accused of interfering in Western politics, which further fueled tensions [28], p. 4. Due to previous Russian aggression against Crimea and Ukraine, Western parties were suspicious of Russia and potential destabilizing actions and training activities. The location of the Zapad exercise was steered near NATO's eastern flank. During previous Zapad exercises, the number of participants was unclear due to different reports from Russian sources (e.g., the Russian MoD). This lack of clarity contributed to insecurity and further suspicion from Western parties.

The fact that the Russian MoD announced 12,700 participants in Zapad 2017, limited the possibility of inspections and observations, since the number of participants was just below the threshold of the Vienna Agreement. This number was believed to be heavily underrated and NATO estimated that in reality 60,000 to 70,000 took part in Zapad 2017 [29].

Some scholars believe that the exercise was designed as an information operation against the West [11] p. 22, [27]. Additionally, an increasing tendency of informational and psychological influencing aspects have been observed in several Zapad exercises [11], p. 24. In his analysis of four Zapad exercises, Petraitis found that each exercise involved events that garnered attention but could not be explained in the West.[5] Different stages and parts of the Zapad operation were tested months before the official date of the exercise as officially announced preparations.[6]

Russia and Belarus held a joint preparatory exercise to Zapad 2017, in which Electronic Warfare (EW) was tested. Several parts of the exercise caused disturbances against other nations such as jamming maneuvers that affected both the Swedish and the Latvian cellular networks as well as the Norwegian air traffic control [30] p. 67, [31], [32].

The majority of the stages in the exercise Zapad 2017 were arranged before the official event.[7] The exercise started earlier than announced and its hidden elements were blended with other military activities in order to

[4] For example, NATO- and NATO-associated exercises increased from 155 to 297 between the years 2014 to 2015.

[5] Zapad exercises held in 1999, 2009, 2013 and 2017.

[6] Usually, four to six months before the official dates.

[7] The majority of the events happened over the 3rd – 7th of July and 4th – 19th of August. The third stage of the official Zapad-17 was held on September 14th – 20th[8] p. 242.

avoid attention. As Petraitis put it: "This approach allows for "undercover" testing of "Zapad operation" activities lasting almost as long as planned or being initiated at a pre-planned time" [8] p. 234.

By showing only a specific part of a "Zapad operation" during a short official period, usually lasting up to one week, Russia could choose to make visible a suitable stage that serves Russia's interests and could be adapted to the security situation [8] p. 234.

It is clear that the Zapad exercises served multiple purposes, in terms of both military and non-military aspects. Apart from testing plans and military forces, strategic communication worked as a tool that affected the security environment. For example, during Zapad 2017 Russia openly showed its willingness to engage in mass defence and actualized the question of nuclear weapons. This sent a message of "[n]ot pushing it into a corner" [8] p. 240. According to Petraitis:

> *The new security situation required the exercise to be used for strategic messaging again, therefore, as soon as the first two aggressive stages had been exercised; it was in the interests of MOD to demonstrate a defensive stage. Emphasizing transparency and openness as their main motives, the MOD invited journalists and observers from other countries to observe part of the official Zapad* [8] p. 242.

In summary, most parts of Zapad 2017 were conducted before the official date in order to conceal offensive operational elements and adjust the exercise according to the security situation. However, the effects of some of the hidden elements in the exercise (i.e., EW) caused disturbances in the neighboring states. The strategy of concealing parts of the exercise and publishing different information about the military training activities leaves room for maneuver and exclusion of other parties. Furthermore, the exercise made it possible to integrate Belarusian and Russian armies further and increase the presence near NATO's Easter border.

2.4.4 Zapad 2021

Geographically, Zapad 2021 was arranged in the Baltic Sea area, at nine ranges in Russia and five ranges in Belarus between 10 – 16 September [24]. Around 2,500 Russian service members were deployed to Belarus for the exercise [33]. In addition to Russia and Belarus, some of the participating forces were represented by India and Kazakhstan. Military observers from the armed forces of China, Vietnam, Myanmar, Pakistan and Uzbekistan were also invited to join the exercise [33]. It could be noted that this was the first time that Kazakhstan was invited to join Russia and Belarus in complex assignments such as nighttime airdrop missions [24].

Zapad 2021 was held in two stages. During the first stage, Russian and Belarusian forces practiced defence against a fictitious aggression directed against Belarus. The second stage included other friendly states, focusing on command and control of the forces in order to restore the territorial integrity of the Belarusian state [33]. The Russian Major General, Yevgeny Ilyin, underlined that Zapad 2021 had purely defensive intentions and expressed:

> *I would also like to draw your attention to the fact that within the framework of the Russian voluntary initiative to remove the areas of large-scale exercises from the Russia-NATO contact line, the main practical actions of the troops will be carried out on the territory of the Russian Federation at a considerable distance from the Western border of the state.* [33]

According to spokespersons from the Russian MoD, Zapad 2021 did not have a specific simulated enemy [33]. However, a Western interpretation was that NATO and the West were the adversaries in the Zapad scenario. Additionally, Western countries were not invited to join or observe the exercise [35].

Zapad 2021 was held in a context of an evolving security situation, drawing attention to Eastern Europe and Belarus. Almost a month before the exercise took place, the Belarusian president Aleksandr Lukasjenko

threatened to organize a migration flow from the Middle East to Europe as a consequence of the European Union (EU) and other European representatives' alleged interference in Belarusian affairs [36]. Additionally, long-term tensions between Western parties, NATO and Russia continued [37]. It has been argued that Zapad 2021 was used as a way to increase military presence and put pressure on the neighboring countries, and the NATO members Poland and the Baltic States (for example, Hurt [38] or Muzyka [39]). These nations were also under significant pressure when the Belarusian threat of migration flow was realized [40].

The exercise raised concern from several European countries [33]. NATO urged Russia to be more transparent with information about Zapad 2021 due to the previous underreporting of data on the number of participants during Zapad 2017 [41]. The Russian MoD clearly stated that several preparatory exercises would be conducted before Zapad 2021, in order to train parts of the resources. About 760 pieces of combat hardware, including 290 tanks and 240 cannons, rocket launchers and mortars, and up to 15 ships and some 80 planes and helicopters were incorporated in the exercise [33].

According to Russian media outlets, about 200,000 troops participated, which meant a significant higher number of participants compared with the official information about previous exercises (e.g., Zapad 2009 and Zapad 2017) [33]. Like Zapad 2017, the exercise held in 2021 contained efforts to manage EW. In this case, a fictitious adversary caused disturbances on navigation and radio communications [33]. In contrast to Zapad 2017, however, the Zapad 2021 scenario did not involve nuclear matters [39].

The relationship between Russia and Belarus appears to be growing stronger, since the joint communication of the military cooperation was introduced early and the exercise was announced as a Belarusian and Russian exercise [37]. It has also been suggested that Zapad 2021 confirmed the high level of military integration between Russia and Belarus [39]. At the same time as Zapad 2021 was taking place, Russia held a parallel exercise. The Russian Northern Fleet ran comprehensive maneuvers in the Arctic, which included 8,000 service members, some 120 airplanes, helicopters and 50 ships [33].

To sum up, Zapad 2021 garnered attention among Western parties due to the tense security situation and the fact that the exercise was the largest strategic exercise compared to previous Zapad exercises. Zapad made it possible to further integrate the Belarusian and Russian Armed Forces and perform in unison. Additionally, the exercise could be seen as a Russian statement of politically supporting Belarus and the rhetoric concerning the migration situation. Finally, Russia showed the ability to run parallel exercises in several directions, from North to East.

2.4.5 Russian Activities During NATO's Military Exercise

NATO's strategic exercise Trident Juncture 2018 (Trje 18) took place October 25 to November 7 in Norway, at the surrounding areas of the North Atlantic and the Baltic Sea. It also included Iceland and the airspaces of Sweden and Finland. The exercise involved all NATO members and the non-members states Sweden and Finland. Trje 18 was based on an article 5 scenario and the joint defence of Norway. Around 50,000 participants from NATO and partner countries joined the exercise and, additionally, around 250 aircraft, 65 vessels and up to 10,000 vehicles were used [42].

Trje 18 exemplifies how Russia responds by military and non-military means. The tensions between Russia on one side, and NATO and the West on the other, intensified when NATO proclaimed that Trje 18 was going to be the largest in recent years [42]. The exercise was criticized by spokespersons of the Russian MoD. The Head of the Russian MoD stated that NATO's activity near the Russia's borders was considered to be "[t]he most intense since the times of Cold War and that exercises are simulations of offensive military activities". Furthermore, the reactions to the exercise were prompted by the fact that Russia's neighbors Sweden and Finland sought closer relations with NATO and joined the exercise without being NATO members. Russia also announced that they were going to conduct their own military exercises near the coast of Norway [43].

At the end of October during Trje 18, the participants experienced trouble with scrambled GPS signals. Norway's defence intelligence agency traced the GPS jamming[8] to a military base near Kola Peninsula. Finland's military intelligence confirmed that the GPS signals were traced to Russia [44].

According to the Norwegian defence minister at the time, Frank Bakke-Jensen, Russia was exercising close to the Norwegian border, and he draw the conclusion that the disturbances were intentional. A number of actions followed the GPS disturbances on the political and informational domains. Complaints from both Norway and Finland were addressed to Russia, due to the negative consequences of the GPS disturbances, which affected both military and civilian planes that were using Finnish air space. Russia responded by asking for evidence to prove the accusations. The Norwegian defence intelligence agency distributed the results of their work with tracking GPS jamming to Russia [44].

However, the Russian Minister of Foreign Affairs dismissed the criticism and labeled it as fantasies. The Minister also expressed that neighboring countries are following a trend initiated by the British Prime Minister Theresa May of inculpating Russia [45]. Moreover, the Finnish Minister of Foreign affairs, Timo Soini, went to Moscow for a meeting with the Russian counterpart to discuss the GPS disturbances. After dialogs between the Minsters of Foreign Affairs in Finland and Russia, and meetings with the Russian embassy, Finland made a statement that the problem was resolved by diplomacy [46].

In a written letter on the Russian MoD's website, the Russian Minister of Foreign Affairs focused very little on the main questions of the GPS disturbances and instead emphasized Russia's close relations and cooperation with Finland [45]. For example, some of the keywords in the article presents the relationship as "neighbors", which gives an impression of closeness. Another viewpoint that the Russian spokesperson brought up was the involvement in trading and the importance of cooperation in this sense (for example, the Finnish energy company Fortum had investments in thermal power plants for heating in Russia during that period).[9]

Moreover, the Russian Minister expressed its skepticism about Sweden's and Finland's participation in NATO's military exercises handling article five scenarios. Russia mentioned "trust", and highlighted Finland's role as a neutral and stabilizing factor in the Baltic Sea area and especially in the North. Russia complained about "Russophobia" and expressed that Russia often is the target of accusations for security problems [45]. Jamming the satellite based navigation system during Trje 18 in Norway and Finland exposed weaknesses in both states. The GPS disturbances in the Norwegian air space have been noticed as a serious problem by the Norwegian Government. This has led to a proposition of measures such as finding alternative systems and reducing dependence on the GPS system [47].

A number of conclusions can be drawn from the section above. Russian criticism of NATO in the informational domain was followed by military actions such as exercises and GPS disturbances. The GPS disturbances during Trje 18 might be referred to as EW. GPS jamming during Trje 18 affected both the exercise and civilian air traffic, which meant that the disturbances were quite successful from a Russian point of view. The actions targeted vulnerabilities in the communication and navigation system, which is a significant matter both within states and between allies.

2.5 ANALYSIS

Based on the analytical concept involving the notions of frontstage and backstage acting, this chapter analyzes Russian behavior during the Zapad exercises and Russian counter actions during NATO's Trje 18. The chapter is structured according to the concepts of legitimacy, mystification and discursive effects.

[8] Disturbances against the Global Positioning System (GPS).

[9] Because of the Russian invasion in Ukraine in 2022, Fortum decided to exit the investments in Russia.

2.5.1 Legitimacy and Political Frontstage Acting

There are at least three strategies with which Russia previously sought to legitimize military actions: formal agreements, information campaigns and the construction of illusions. Seen from the political frontstage, formal agreements such as the Vienna Document 2011 on confidence and security building measures, work as a symbol for cooperation and transparency in Europe.

The process of establishing legitimacy during the Zapad exercises included an early information campaign with the release of public information about the exercise, which was constructed in order to give a wide audience an impression of transparency. The announcement of the Zapad 21 exercise was communicated in a political setting by the Russian MoD almost a year before the active phase of the exercise began. The information published by the MoD described preparatory exercise activities that would take place on different months. Certain parts of the information was connected to the Vienna Document 2011 and included an announcement on the number of participants who planned to take part of the exercise [33]. Official reports were regularly published (by the MoD and Russian media outlets) so that the audience was updated with messages about the exercise. The military performance was thus coordinated with the political and the information domain.

Well aware of the tense security situation, a Russian Major General expressed that Russia would voluntarily keep the major part of the exercise far from the NATO border [33]. This might be seen as a way of justifying the location of the exercise and dampening concerns from Western parties. However, it could be argued that the efforts to legitimate the Zapad exercises are a construction of illusion due to Russian failures to follow formal agreements and share information.

2.5.2 Cracks in the "Legitimate" Facade

Even though legitimate strategies are initiated by Russia, there are some cracks in the legitimate facade. Russia has been criticized for violating parts of the agreement in the Vienna Document 2011 in its actions in Georgia and Ukraine. OSCE has suggested that the Vienna Document 2011 needs to be updated due to technological changes, the security situation, and the existence of new military capabilities such as Unmanned Aerial Vehicles (UAV) [48].

When comparing four of the previous Zapad exercises, Petraitis found that Military Commanders spoke openly during the earlier Zapad exercises (1999 and 2009) but during the later ones (held in 2013 and 2017) revealed less information. In other words, there was a tendency for information and speeches to become more closed [8]. Western parties have criticized Russia for unclear communication concerning the number of participants in exercises due to previous issues and for not following the agreements.

Politically, Russia has accepted the Vienna Document 2011 on being transparent with exercises and military activities but has been critical to the need of an update on the agreement [49]. The Vienna Document may be an important setting in the political domain to preserve a legitimate facade. However, the agreement was clearly broken during the Russian military exercises and operation near the Ukrainian boarder on 24 February 2022.

2.5.3 Backstage Acting and Mystification

The notion of mystification refers to information that is accessible to a selected organization or group, and that offers a position of power vis-à-vis other parties who are excluded [18] p. 9. As mentioned in the theoretical chapter, indications of hidden information may lead to greater awareness and interest among excluded parties [18] p. 9. Mystification appears connected to backstage acting due to the widespread interest in Russia's actions behind the scenes. This interest might be explained by the security situation in 2021, in which Russia's aggression against Ukraine and the incompatibilities between NATO and Russia were of importance.

The security situation demonstrates a need to understand what Russia does and what Russian intentions are. The fact that most parts of the Zapad exercises are conducted "backstage", that information is lacking and that Western observers are excluded leads to the phenomenon of mystification. This does not mean that other states must know everything that Russia does when they are testing plans or hold their military exercises. The point is that Russia's aggressions and their tendency towards backstage acting creates a relation in which excluded parties have a constant need to know.

Most parts of the Zapad exercises in 2017 and 2021 were conducted backstage, while the military performance was visible "on stage" during a couple of weeks. Over the course of these exercises, Russia and Belarus have increasingly come to perform as "The Union" with joint communication. At the same time, information about the events were rare. As a result, Western parties have been placed in the position of "information seekers" in order to be able to interpret Russian and Belarusian intentions and capability. From this perspective, Russia and Belarus hold the role of "information owner". During both Zapad 2017 and Zapad 2021, media coverage was extensive and offered information and speculations about the exercises. Furthermore, the combination of the "information seekers" lack of information and wide interest might lead to susceptibility for disinformation and myths.

Russia and Belarus use strategies to conceal parts of their military activities and take advantage of the gaps in the Vienna Document 2011. Heuser describes how in some cases parties break down the exercises into smaller components as a way of overcoming the requirement to announce to the OSCE when the number of participants exceeds 9,000 [12] p. 25. In Russia's case, the Zapad exercises contained smaller exercises that were labeled "rehearsals" or preparatory training, which is a way of acting backstage in both the military and political domain.

2.5.4 Military Aspects of Frontstage and Backstage Acting

Analyzing military exercises through the lens of backstage and frontstage acting shows that Russian strategic exercises have multiple purposes and effects. In terms of the military domain, it is clear that parts of the exercises are visible frontstage when it serves certain purposes, whereas the exercises also include backstage acting when needed.

The structure and organization of strategic exercises in a year-long cycle might give an illusion of a visible repetitive pattern, but most part of military exercises are conducted backstage. The use of backstage acting means that Russian military resources are active in extensive training activities and cover the geographical area in the Baltic Sea during a longer period of time than announced. Exercises are well synchronized with discursive strategies when Russia seeks to convince its audience on the frontstage. The effects might be powerful depending on the security situation and the susceptibility of the audience.

Another aspect when it comes to the military dimension of frontstage acting is the upgraded military district in Northern Europe [14]. This initiative indicates two things: a growing interest in the northern part of Europe and the Arctic, as well as a military rebuilding and a higher security thinking against Western states and NATO. The parallel exercise in the North also shows the ability to run several operations and the potential threat that Russia might see in those directions. At the same time, Russia's support to Belarus amid security issues such as allegations of Belarusian organization of migration flow during 2021 could be seen as a political statement. In this way, a military exercise such as Zapad 2021 became a political tool with significant potential to influence an already tense security environment, especially in Eastern Europe.

2.5.5 Discursive Effects

In this context, the notion of discursive effects refers to how Russia produces knowledge and power within the military discourse. Russia is active on both the political and military scenes and uses information channels to produce knowledge within the military discourse. One way of gaining power is via the position of "information

owner". As discussed in a previous section, in such cases communication might garner more attention. During Trje 18 Russia used different strategies in order to affect the opposite side. These methods included:

- Construction of NATO as a security threat;
- Confrontational strategies;
- Accusations; and
- "Playing the relation card".

Trje 18 offers an example of how Russia performs in the political, informational and military dimensions. The initiation of frontstage acting appeared in political statements made by spokespersons from the Russian MoD. The discursive construction of NATO conjured an image of a security threat in North Europe. This strategy created a view of NATO as an offensive force in Russia's vicinity that "forced" Russia to consider its defence. The strategy functioned as a way of legitimating Russia to initiate their own military exercises.

Russia openly reacted to the size of the Trje 18 arrangement when referring to the exercise in terms of "the most intense since the times of Cold War." It could also be noted that Russia describes exercises "as simulations of offensive military activities", in negative terms.

During Trje 18, Russia specifically denounced and questioned the fact that the neighboring states Sweden and Finland took steps towards a closer relationship with NATO by participating in the exercise. This argument discursively positioned NATO as a military force that interferes in the North and demonstrated that Russia does not accept that neighboring states engage with NATO. This could be compared to Herta's conclusions in her study about how ideational element, such as the construction of an alternative reality in the information domain, affects opinions and creates a picture that is in line with Russian aims. In this way, ideational aspects can be used as a "force multiplier" [1] pp. 68-69. A number of analysts argue that Russia's statement was a political signal to Sweden and Finland to refrain from tightening relations with NATO [43]. When Russia was confronted, the strategy was to counter with accusations against other nations and politicians, and to complain about "Russophobia" [45]. As a result, Russia placed itself in a subordinated position as a target of accusations.

At the frontstage, Russia did not accept the behavior of others, such as the "intense military activity". However, Russia initiated a powerful performance by stating that Russia would arrange its own military exercises near Norway during Trje 18. Russia managed to conduct backstage activities that affected interoperability within NATO's exercise. The EW was successful in several ways: vulnerabilities among neighboring states were identified or confirmed and interoperability between the participants in Trje 18 was negatively affected. Furthermore, the weaknesses were questioned and exposed in media. Efforts by Nordic states to clarify the disturbances with Russia were unsuccessful but were exposed in media during several years. In that way, the GPS jamming resulted in long-term effects in both the political and informational domain.

Relational aspects are of importance and, in the case of Trje 18, the complexity might be seen as high due to the geographic proximity between the Nordic states and Russia. Political efforts to handle the disturbance problem were challenged by confrontational strategies met by Russia. Russia's demands for proof of the accusations of the GPS disturbances were met, but never accepted. Instead, the accusations were labeled as fantasies [45].

As an answer to the accusations of the GPS disturbances Russia used the strategy "playing the relation card", which means taking advantage of the relation and geographic closeness to one of the Nordic countries. In political statements on the Russian MoD, the Minister of Foreign Affairs, referred to the joint business projects with Finland. The Minister especially emphasized the close relation between Russia and Finland. By using this strategy, Russia constructs a narrative of a close relation with Finland, which abates the argument that Russia uses EW against a neighboring state. The effect of this strategy is that the official

argumentation is overshadowed and the accusations fade out. In this way, Russia uses power instruments in order to influence and reach for discursive effects. An interesting perspective, however, is that the problem was officially solved with diplomacy behind closed doors, in other words, backstage.

2.6 CONCLUSION

In this case study, Zapad 2017, Zapad 2021, and Russian behavior during NATO's strategic exercise Trje 18 have been analyzed through the lens of frontstage and backstage acting.

Russia's frontstage acting is integrated into the political and military dimension as well as the informational. The military performance during the Zapad exercises took place openly during a short time frame, while most of the exercise activities remained hidden. Frontstage acting is performed within a political context in order to legitimate and send messages about a planned exercise. Depending on the security situation and Russian aims, the frontstage acting performed by Russia is adjusted to fit its purposes. Still, frontstage acting may be used to construct threats and address critique against a competitor.

Military and non-military actions connected to Zapad 2017 and Zapad 2021 indicate larger exercises, a stronger establishment of the Union between Belarus and Russia, and the capability to run parallel exercises in several directions that cover a wider geographical area. Military, political, and informational dimensions are interconnected and complement each other and activities in one dimension may be increased at a certain point in time if it is deemed suitable. The example of Russian counter actions during NATO's strategic exercise in the Baltic Sea area together with non-NATO members demonstrates how activities are intensified in the military dimension as well as the political and informational dimension. In response to NATO's presence, Russia carried out its own military exercises and increased informational activities in order to construct the image of NATO as a security threat in Europe.

During NATO's strategic exercise Trje 18, Russia performed both frontstage and backstage. Provoked by NATO forces in its vicinity, Russia used the political scene to criticize NATO for posing a security threat. At the same time, Russia acted backstage by EW, causing effects on both vulnerabilities in the civilian airspace and disturbances of the communication system within NATO's exercise. These initiatives could be seen as ways of demonstrating Russia's power and ability to affect its adversary.

Exercises might be visible if Russia chooses frontstage acting or invisible when Western parties are excluded and backstage activities are conducted. In that way, exercises have a relation building aspect, in which an actor or actors have the power to include or exclude other parties. In a security situation characterized by tensions and incompatibility, this inclusion and exclusion may further fuel friction. The Russian exercises are flexible in intensity, rhythm and complexity and they are functioning as communicative instruments. The findings suggest that the role of exercises and their effects in different domains should not be underestimated and that strategic exercises are versatile because of the possibility of using them in various ways.

Since the onset of the Russian war on Ukraine in 2014, the military presence in the Baltic Sea area has been noteworthy, as both NATO and US have increased their activities in the geographic zone. Because of the security political tensions and the increased military activities, potential consequences of multinational military exercises in the Russian zone of operations conducted by the Western parties, must be analyzed and considered in planning processes. Coordination and communication between US, NATO and non-NATO members is important when organizing the military in order to avoid unintended consequences and instead reach desired conditions. The research, analysis, and drafting of this chapter occurred prior to Russia's full invasion of Ukraine in 2022. As could be expected, Russia has not held broad strategic level joint combined military exercises since that time. Nevertheless, Russia has continued to react to NATO exercises, and it should be expected that Russia will, at some point in the future, resume larger exercises as it reconstitutes its military forces, regardless of the outcome of its war against Ukraine.

2.7 REFERENCES

[1] Herta, L. "Russia's Hybrid Warfare – Why Narratives and Ideational Factors Play a Role in International Politics." On-line Journal Modelling the New Europe 21, 2016.

[2] Bachmann, S.D. and Gunneriusson, H. "Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security." Scientia Militaria, South African Journal of Military Studies, 43(1), 2015, pp. 77-98. Doi: 10.5787/43-1-1110.

[3] Giles, K. "Russia's 'New' Tools for Confronting the West, Continuity and Innovation in Moscow's Exercise of Power". Research paper. Russia and Eurasia Programme, March 2016. https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf Accessed 10 November 2023.

[4] North Atlantic Treaty Organization, NATO. "Research Specialist Team on Hybrid Warfare: Ukraine Case Study." AC/323(SAS-121)TP/729, STO-TR-SAS-121. NATO Science and Technology Organization, Neuilly-sur-Seine, France, 2018.

[5] North Atlantic Treaty Organization, NATO. "Hybrid Warfare: Implications for NATO." AC/323(SAS-127)TP/792, STO-TR-SAS-127. NATO Science and Technology Organization, Neuilly-sur-Seine, France, 2018.

[6] Aronsson, A., and Ottosson, B. "Western Military Exercises 2014-2019 – Adjustment, development, and progress." FOI-R—4875--SE. The Swedish Defence Research Agency, 2020.

[7] Norberg, J. "Training for War. Russia's Strategic-level Military Exercises 2009 – 2017." FOI-R--4627—SE, The Swedish Defence Research Agency, 2018.

[8] Petraitis, D. "The Anatomy of Zapad-2017: Certain Features of Russian Military Planning." Lithuanian Annual Strategic Review 2017 – 2018, 16. Military Academy of Lithuania. The General Jonas Žemaitis Military Academy of Lithuania, 2018. ISSN 2335-870X. DOI: 10.2478/lasr-2018-0009.

[9] Kuo, R., and Blankenship, B. "Deterrence and Restraint: Do Joint Military Exercises Escalate Conflict?" Sage. Journal of Conflict Resolution 1(29), 2021. https://journals.sagepub.com/doi/full/10.1177/00220027211023147

[10] Wolfley, K.J. "Military Statecraft and the Use of Multinational Exercises in World Politics." United States Military Academy. West Point Research Papers, 2019. https://academic.oup.com/fpa/article-abstract/17/2/oraa022/6123995?redirectedFrom=fulltext

[11] Ventsel, A., Hansson, S., Madisson, M-L., and Sazonov, V. "Discourse of Fear in Strategic Narratives: The Case of Russia's Zapad War Games." Media, War and Conflict 2021, 14(1), 2021, pp. 21-39. Sage. DOI: 10.1177/1750635219856552.

[12] Heuser, B. and Simpson, H. "The Missing Political Dimension of Military Exercises." The RUSI Journal, 162(3), 20-28, 2017. DOI: 10.1080/03071847.2017.1345118.

[13] Ferris, E. "The True Purpose of Russia's Zapad Military Exercises: Why Moscow Wanted to Send a Message to Minsk." 2017. Foreign Affairs, 04 October 2017. https://www.foreignaffairs.com/articles/russia-fsu/2017-10-04/true-purpose-russias-zapad-military-exercises Accessed 12 January 2022.

[14] Congressional Research Service, CRS. "Russian Military Exercises." CRS reports for the United States Congress, October 2021. https://crsreports.congress.gov/product/pdf/IF/IF11938 Accessed: 13 November 2021.

[15] Noble, T. and Pym, B. "Collegial Authority and the Receding Locus of Power." British Journal of Sociology 21(4), 1970.

[16] Organization for Security and Co-Operation in Europe, OSCE. "Vienna Document 2011. On Confidence – and Security Building Measures." OSCE, 2011.

[17] Organization for Security and Co-operation in Europe, OSCE. "Progress on Modernizing the Vienna Document Vital to Making the Agreement Effective in Current Challenging Security Environment." 1 February 2017. https://www.osce.org/fsc/296801. Accessed 15 December 2021.

[18] Wodak, R. The Discourse of Politics in Action. Politics as Usual. Palgrave Macmillan, New York, 2009. ISBN-978-0230-01881-5.

[19] Goffman, E. The Presentation of Self in Everyday Life. Anchor, 1959. ISBN: 9780385094023.

[20] Saurugger, S. "Constructivism and Public Policy Approaches in the EU: From Ideas to Power Games." Journal of European Public Policy 20(6), 2013, pp. 888-906. Routledge. Taylor& Francis Group. DOI: http://dx.doi.org/10.1080/13501763.2013.781826.

[21] Foucault, M. Power Knowledge. Selected Interviews and Other Writings, 1972 – 1977. Random House USA Inc., New York, 1988. ISBN:9780394739540.

[22] Kjellén, J. "The Russian Baltic Fleet-Organization and Role within the Armed Forces in 2020." FOI-R--5119--SE. The Swedish Defence Research Agency, 2021.

[23] Collective Security Treaty Organization, CSTO. The CSTO Structure. 2021. https://en.odkb-csto.org/structure/ Accessed 09 December 2021.

[24] Interfax America, Inc. "Newly Independent States; Paratroopers Airdropped from Il-76MS Planes at Brest Range During Zapad 2021 Exercise." Moscow, 17 September 2021b. Accessed 10 December 2021.

[25] The Russian Ministry of Defence, MoD. "Zapad 2017 Joined Strategic Exercise." 2017b https://eng.mil.ru/en/mission/practice/more.htm?id=12140115@egNews Accessed 12 January 2022.

[26] The Russian Ministry of Defence, MoD. "Russian Defence Minister Summed up Zapad 2017 Exercise." 2017a. https://eng.mil.ru/en/news_page/country/more.htm?id=12145455@egNews. Accessed 12 January 2022.

[27] Wilk, A. "The Zapad-2017 Exercises: The Information War (For Now)." Centre for Eastern Studies, No.249, 01 September 2017. OSW Commentary. https://aei.pitt.edu/89837/. Accessed 10 November 2023.

[28] University of Pittsburgh. Stockholm International Peace Research Institute, SIPRI. SIPRI Yearbook 2018. Armaments, Disarmament and International Security, 2018.

[29] Johnson, D. "Zapad 2017 and Euro-Atlantic Security. NATO Review." NATO, 14 December 2017. https://www.nato.int/docu/review/articles/2017/12/14/zapad-2017-and-euro-atlantic-security/index.html Accessed 12 December 2021.

[30] Kjellén, J. "Russian Electronic Warfare. The Role of Electronic Warfare in the Russian Armed Forces." FOI-R--4625--SE. The Swedish Defence Research Agency, 2018.

[31] Birnbaum, M. "Latvia's Cellphones Stopped Working. Russia's War Games May Be to Blame." 2017. The Washington Post. Published 5 October 2017. https://www.washingtonpost.com/world/europe/latvias-cellphones-stopped-working-russias-war-games-may-be-to-blame/2017/10/05/449162d4-a9d3-11e7-9a98-07140d2eed02_story.html Accessed 09 November 2021

[32] Nilsen, T. "Electronic Warfare. Norway Well Prepared to Meet Russian Jamming." 2017. The Barents Observer. 14 September 2017. https://thebarentsobserver.com/ru/node/3327 Accessed 09 November 2021.

[33] The Russian Ministry of Defence, MoD. "News – Zapad 2021." 1 September 2021e. https://eng.mil.ru/en/news_page/country/more.htm?id=12381644@egNews Accessed 21 January 2024.

[34] The Russian Ministry of Defence, MoD. "Main Directorate of International Military Cooperation of the Ministry of Defence of the Russian Federation Holds Briefing on Preparation of Zapad 2021 Joint Strategic Exercise." 20 August 2021d. https://eng.mil.ru/en/news_page/country/more.htm?id=12378427@egNews Accessed 17 January 2022.

[35] Center for European Policy Analysis, CEPA. "Russia's Zapad 2021 – Lessons Learned." 2021. https://cepa.org/russias-zapad-21-lessons-learned/ Accessed 16 December 2021.

[36] Atlantic Council. "Belarus Dictator Escalates EU Border Migrant Crisis." 2021. https://www.atlanticcouncil.org/blogs/belarusalert/belarus-dictator-escalates-eu-border-migrant-crisis/ Accessed 16 December 2021.

[37] The Moscow Times. "Zapad 2021: What We Learned from Russia's Massive Military Drills." 2021. https://www.themoscowtimes.com/2021/09/23/zapad-2021-what-we-learned-from-russias-massive-military-drills-a75127. Accessed 16 December 2021.

[38] Hurt, M. "Is Zapad 2021 Any Different from Zapad 2017?" International Centre for Defence and security, ICDS. Estonia, 14 September 2021. https://icds.ee/en/is-zapad-2021-any-different-from-zapad-2017/. Accessed 17 January 2022.

[39] Muzyka, K. "Defending the Union. Zapad-2021." International Centre for Defence and security, ICDS. Estonia, December 2021.

[40] BBC News. "Poland Border Crisis: What Happens to Migrants Who Are Turned Away?" 2021. https://www.bbc.com/news/59348337 Accessed 26 January 2022.

[41] Emmot, R. "NATO Calls on Russia to be Transparent with Russian Military Exercises". Reuters. 03 September 2021. https://www.reuters.com/world/nato-calls-russia-be-transparent-with-military-exercises-2021-09-03/ Accessed 09 November 2021.

[42] North Atlantic Treaty Organization, NATO. "The Secretary General´s Annual Report 2018." 2019.

[43] Warsaw Institute. "Russia Reacts to Trident Juncture 18." Baltic Monitor, 1 November 2018. https://warsawinstitute.org/russia-reacts-trident-juncture-18/ Accessed 16 December 2021.

[44] Axe, D. "GPS Jammed Russia Messing Americas F-35s." The National Interest, October 2019. https://nationalinterest.org/blog/buzz/gps-jammed-russia-messing-americas-f-35s-90136 Accessed 9 November 2021.

[45] The Russian Ministry of Defence, MoD. "Foreign Minister Sergey Lavrov's Comments and Answers to Media Questions During the Joint News Conference Following Talks with Foreign Minister of the Republic of Finland Timo Soini." Moscow, 12 February 2019. https://www.mid.ru/en/web/guest/meropriyatiya_s_uchastiem_ministra/-/asset_publisher/xK1BhB2bUjd3/content/id/3513560. Accessed 10 November 2021.

[46] Lindroos, I. Efter ryska GPS-störningar-så här svarar utrikespolitiker om hur såbart Finland är ["After Russian GPS Interference – Here's How Foreign Policy Responds to how Vulnerable Finland Is."] Svenska Yle, 22 November 2018. https://svenska.yle.fi/artikel/2018/11/22/efter-ryska-gps-storningen-sa-har-svarar-utrikespolitiker-om-hur-sarbart-finland. Accessed 10 November 2021.

[47] Norwegian Government. Proposisjon til Stortinget Prop.1 S, 2019-2020 ["GPS-Jamming."] https://www.regjeringen.no/no/dokumenter/prop.-1-s-20192020/id2671512/?q=GPS-jamming&ch=2#match_0). Accessed 10 November 2021.

[48] Organization for Security and Co-operation in Europe, OSCE. (2017). "Progress on Modernizing the Vienna Document Vital to Making the Agreement Effective in Current Challenging Security Environment." 01 February 2017. https://www.osce.org/fsc/296801 Accessed 15 December 2021.

[49] Ra, S.-H. Svenska Yle. Norge lade fram karta över ryska gps-störningar-Fantasifullt, säger Sergej Lavrov ["Norway Presented Map of Russian GPS jamming. 'Imaginative,' says Sergei Lavrov."] 12 February 2019. Accessed 09 November 2021.

Chapter 3 – RUSSIAN INFLUENCE ACTIVITIES ON, AND IN, KOSOVO

Dorthe Bach Nyemann and Jeanette Serritzlev
Royal Danish Defence College
DENMARK

3.1 INTRODUCTION

This chapter provides a case study on Russian influence activities on Kosovo. In doing so, it contributes to a deeper understanding of how Russia tailors its activities to different regions and geopolitical realities. The case study details Russian influence activities in Kosovo and possible consequences for NATO.[1]

3.1.1 Initial Scope and Research Question

The initial idea for the case study was to uncover Russian information activities targeting KFOR personnel, specific KFOR missions in Kosovo, and the overall NATO presence in the area. We also intended to scrutinize how KFOR personnel prepare for and respond to these activities. Two primary hypotheses guided our initial perceptions. Firstly, we expected that Russia would exploit a lack of mutual trust in the Kosovo community, horizontally and vertically, intending to stop local progress and display NATO's inabilities as a provider of security and normalization in Kosovo. Secondly, we expected that KFOR would react to activities from Russia without a shared situational awareness or a collective toolbox to respond. We furthermore expected KFOR's responses to be ineffective, rely on individuals' actions, and not deter Russia and Serbia from taking additional steps. With this as our point of departure, we asked the following question:

> *What is the scope of Russian information activities affecting the KFOR mission and ability to operate, and what is KFOR's response to these activities?*

However, we have realized that this scope is too narrow when looking at Kosovo. We need a broader perspective to unpack Russian initiatives designed to disrupt positive developments in Kosovo and the NATO mission. We discovered that the situation in Kosovo is incomparable to that of, e.g., the Baltic states, where direct influence operations from Russia towards NATO personnel are continuously detected [1] pp. 8-9, [2]. It is also very different from other areas of Russian interest, e.g., Ukraine or Syria. We have learned to apply a much larger lens to understand the Kosovo case, including Serbia and related areas where Serbian minorities live. We will argue that Kosovo and the KFOR mission must be approached analytically as only one small part of a larger puzzle. Kosovo is only one piece of the "Serbian World," where Russia and Serbia have corresponding interests. The "Serbian World" is a concept we will explain in more detail in the report. We will argue that Russia continuously supports Serbia through many means and channels. Viewing Russian activities through a lens of preserving a "Serbian World," it becomes essential to distinguish between Russian influence ***on*** the fate of Kosovo as an independent state and Russian influence activities ***in*** Kosovo itself.

This report argues that Russia is very active ***on*** the Kosovo question; however, examples are few, scattered, and lack intensity regarding influence activities ***in*** Kosovo. Russia seems to play a minimal role in Kosovo and even less in disturbing KFOR's day-to-day tasks among the Kosovo population. The report will unpack this argument through documentation from our sources. It will argue why this is the most rational position for Russia, and it will also discuss what this means for the KFOR mission and NATO reactions.

[1] The collection of data and information for this case study concluded in December 2022.

3.2 METHODOLOGY

In preparing for our field study tour to Kosovo, we have collected data through an extensive search on literature regarding developments in Kosovo and the West Balkan region more broadly. Furthermore, during the fall of 2021, we conducted group interviews and individual interviews with Danish officers who have served in the KFOR mission during the last five years with specific tasks regarding PSYOPS operations in HQ KFOR.[2]

After this initial phase, we went to Kosovo in November 2021 to gather further information. In Kosovo, we had in-depth interviews with three NGO community representatives who provide the government in Kosovo with political analysis and advice but have stayed independent of government funding, depending instead on a wide range of Western donors. The three interviewees represented the organizations: Kosovar Centre for Security Studies (KCSS), Kosovar Institute for Policy Research and Development (KIPRED), and Kosovar Democratic Institute (KDI). Through our interviews, we also received additional written material to our benefit. Additionally, we interviewed personnel from the KFOR mission and NATO regarding their experiences with Russian influence in Kosovo during our stay, moreover, we followed a Danish Tactical PsyOps Team on patrol to some Serbian enclaves.

Our research in Kosovo gave us a broader understanding of how NATO contributes to stable conditions in Kosovo and how the situation in Kosovo is currently perceived. Experiencing Kosovo on our own has provided us with many nuances to our original views on Russia's role and activities in Kosovo and our understanding of the role and possibilities for KFOR and NATO in the area. Before we dive into the analysis of the Russian approach to influence in and on Kosovo, we will give a short insight into the current security situation in Kosovo, intending to provide an overview of the vulnerabilities that Russia could potentially exploit in an influence operation.

3.3 THE CURRENT SECURITY SITUATION IN KOSOVO

Visitors to Kosovo, who went there 10 or 15 years ago, may have difficulties recognizing the capital in 2022. During our visit in the fall of 2021, we witnessed a capital in rapid expansion with many new buildings and building projects. Talks with our interview respondents, locals, and KFOR personnel supported a general optimism and hope for the future among the population. According to our local respondents, the positive development trends also regard countering religious radicalization and national discord. That does not mean that everything is perfect. Unemployment, corruption, and organized crime are just some of the issues of concern for the citizens. However, the situation in Kosovo is far better than just a few years ago.

3.3.1 Recognition of Kosovo's Independence

As of March 2020, Kosovo is recognized as an independent state by 92 out of 193 UN nations, 22 out of 27 EU member states and 26 out of 30 NATO member states [3], [4] The EU member states not recognizing are Greece, Spain, Slovakia, Cypres, and Romania. To the great regret of Kosovo, eighteen states have withdrawn their initial recognition of Kosovo in the last few years; these include countries like Burundi, Central African Republic, Dominica, Grenada, Guinea Bissau, Lesotho, Liberia, Papua New Guinea, São Tomé and Principe, Sierra Leone, and Suriname [5]. Some of these withdrawals are directly related to diplomatic relations with Russia.

[2] Interviews were conducted during the fall of 2021 with former deployed Danish officers to the KFOR mission, with current deployed Danish personnel in the KFOR mission and local academics from academia and think tanks in Pristine.

3.4 POLITICAL SYSTEM

Kosovo has a one-chamber parliament consisting of 120 members, and Kosovo has both a President and a Prime Minister. In February 2021, Kosovo held an election for parliament, where the ruling party became the social democratic party LVV with 50.3 percent of the votes. Not surprisingly, the ethnic challenges are also reflected in the political environment with different ethnic groups. Srpska Lista (Српска листа) is the dominant political movement for Serbian minorities. According to the constitution, ten seats in the Kosovo Assembly are guaranteed for Serbs and another ten for other minority communities, including Ashkali, Bosniaks, Egyptian, Gorani, Roma, and Turks [6] p. 8. Srpska Lista holds all 10 Serbian mandates [6] p. 5, making it one of the five larger parties in parliament. Additionally, many groups are only represented by one or two members [6] p. 4. Of relevance to our study is that Srpska Lista has ties to Putin's United Russia [7], p. 19. The list has also officially been supported by United Russia [8].

According to a focus group research by NDI [6], p. 6, and also supported by our interviews, the 2021 election is the first election since independence, which marked a change in attitudes toward patriotism. Before the 2021 election, veterans of the 1998 – 1999 war were respected for patriotism and forgiven for acts of crime. Our interview respondents coherently confirmed that UCK (Kosovo Liberation Army) is still respected for their fighting in the war, but this is no longer unconditional. War crimes must be punished, and merits in the past do not mean a free ride for privileges in the present.

3.4.1 General Trust in Authorities and Optimism About the Future

From civilian and military interview respondents, we got a consistent impression of a stable and still improving security situation in Kosovo. As one informant put it: "*In Kosovo, there is no mood for war*." From his perspective, the situation in Bosnia is currently the most worrying in the Balkans. The second most worrying situation is Montenegro, which he characterized as a state "*at the state of conflict*." Furthermore, the same informant stated: "*There is a lot of Russian influence IN Montenegro, and there is a lot of Russian influence ABOUT Kosovo*." Other respondents also supported the statement of Russian influence being more ABOUT Kosovo in our research.

Our interview respondents collectively supported the impression of a Kosovo with still improving institutions, including a Kosovo Police, which is generally accepted and trusted. Acceptance includes the Serbian community, and Serbs also serving in Kosovo Police, as opposed to the situation within Kosovo Security Force. In the Serbian part of Mitrovica, the Kosovo Police Force is all or mainly Serbian – which seems to be a solution satisfying most parties and supporting stability. According to our local respondents, Kosovo Police also has relatively successful campaigns against corruption and extremism.

UCK, The Kosovo Liberation Army is still very present in public life (memorials, billboards, statues, flags). However, a survey from 2021 indicates that there has been a change in attitudes amongst the population. According to the survey, public service and integrity are viewed as keys to patriotism rather than service in the war [6]. Our respondents supported the argument by pointing to the younger population being engaged in prosperity for the future has another view on national identity and does not want it only to be defined by the war. Around 40 % of the people in Kosovo are under 25 years old. This indicates that perceptions of and views on the UCK are divided between an older and a younger generation, and the number of young people significantly impacts changing perceptions.

3.4.2 The Serbian Enclaves

Throughout the political, religious, and cultural sphere, you also find the omnipresent myth of the battle at Kosovo Polje in 1389. In the eyes of the Serbs, Serbian soldiers under the command of King Lazar fought against the Ottoman invaders under the command of Sultan Murat. The Serbs lost the battle but stopped the

Ottomans from further expansion. The Serbian narrative of the battle in 1389 is thus not a narrative of victory but one of bravery and sacrifice. According to legend, King Lazar had a vision the night before the battle. God gave him a choice between an empire on earth or in heaven. King Lazar chose the latter. In the eyes of Serbs, Lazar did the noble thing, taking the sacrifice on his shoulders and rescuing the rest of Europe from a Muslim invasion.

It is out of the scope of this report to go further into the current effects of the narratives of history. Still, it is of absolute necessity to understand that the current political situation and dispute cannot be separated from perceptions of the battle – and the myth – in 1389 (Figure 3-1). The political role of the myth helps explain why it is highly unlikely, at least in the near future, to imagine a Serbian government recognizing an independent state of Kosovo. Furthermore, this is why the situation in the Serbian enclaves in Kosovo is not only about the people living there but also of vital interest to Belgrade.

Figure 3-1: Monument for the Battle in 1389 where the Serbs Fought Against the Ottomans. Private photo from Kosovo Polje in November 2021. Jeanette Serritzlev.

The living conditions in most Serbian enclaves around Kosovo are fairly the same as for the Albanians, with the exception of the northern territories boarding Serbia. The Serbian enclaves, not including the one in the North, are spread around the country as minority communities surrounded by primarily Albanian communities. Unemployment, financial insecurity, and corruption within the system are general areas of concern across ethnicity [6], p. 6. In the North, however, where the river of Ibar splits the city of Mitrovica, the situation is different due to geography and closer direct ties to Belgrade (Figure 3-2). It used to be the Albanian side of Mitrovica that saw growth and wealth when looking to the North. Today the situation has turned around. We learned that the younger generations in the North are fleeing the area due to a lack of work and possibilities. This is, of course, a challenge for Belgrade to hold Serbs in Mitrovica closer to Belgrade. As a countermeasure, Serbia is building settlements for returning Kosovo Serbs [9], [10]. Several respondents told us how the Serb minority in this area was being paid or financially supported directly by Belgrade. Other rumors mentioned Serbia arranging and paying for demonstrations among the Serb minorities on different occasions. However, finding neutral and new sources confirming so in writing has proven difficult. An example of this is an article in BalkanInsight.com from 2008, which mentions that Serbs in Kosovo, allegedly encouraged by the government in Belgrade, quit their jobs for the Kosovo authorities, now protesting against Belgrade, as they had not received the money promised [11].

What is undisputed, though, is the parallel structures, especially in the North, including the Serbian Civil Protection Corps, which was dismantled in 2015. Former servicemen in the corps were transferred to other Kosovo state institutions. This initiative has proven unsuccessful. Employees were paid for years but never showed up to work in the state institutions [12]. The situation is, though, still much more stable than ten years ago. During our stay in November 2021, KFOR drove patrols north of Ibar. Being on one of these patrols, we did not witness any tension or anti-KFOR sentiments. According to the soldiers conducting these patrols, that was aligned with the ordinary situational picture, they experienced.

We learned from our respondents that the citizens in the Serbian part of Mitrovica do not pay for certain supplies like water and electricity. According to a report from 2016, it seems to be a 'non-pay agreement,' meaning that most citizens simply do not pay their bills [13] pp. 12-13. Once again, this is an example of the challenges in finding exact and verified information. However, in conjunction, the examples support that Kosovo has ungoverned spaces with a lack of overall control and monopoly of jurisdiction. Still, the situation overall appears very stable. In the autumn of 2021, a dispute about license plates got a lot of international media attention. In 2016, an agreement was reached in Brussels on provisional arrangements for vehicle license plates. That agreement expired in 2021, and the government of Kosovo announced that "status neutral" license plates without Kosovo insignia would no longer be considered valid. The decision created tension and blockades at two border crossings. Serbian Armed Forces also sent MiG-29 fighter jets in the air and T-72 tanks to the border. The Serbian Minister of Defence visited the border crossings with Serbia's Russian Ambassador [14]. Having studied "License Plate Gate" beforehand, we expected to learn much more during our stay in Kosovo. Surprisingly, our local and KFOR interview respondents did not put much effort into this. As our KFOR respondents expressed consistently, the 'hype' of this case was more about international politics than internal concerns within Kosovo. In October 2021, a deadline was set for Serbian-registered cars to cover Serbian state symbols with officially produced stickers [15]. When we visited the Serbian part of Mitrovica, we found that most of the cars in the city wore those stickers and that the situation at the border crossings was back to normal.

According to our respondents, enclaves in the south seem to have a more positive attitude towards local authorities and KFOR. Mainly Albanian communities surround these enclaves. To our knowledge, the Kosovo Police is not ethnically divided in these parts of the country. According to our respondents, Kosovo Police is acknowledged as a reliable force among both Serbs and Albanians.

The future role and current impact of the Kosovo security situation are more ambivalent to evaluate. Kosovo Security Force (KSF) is now a light-armed force and continues the transformation into a regular armed force. By the current mandate, KFOR and the NATO Advisory and Liaison Team (NALT) [16] can advise on the organization, procurement, etc. Still, KFOR cannot interact in advising on the transformation of KSF to a regular army. It seems reasonable to indicate that this could be an issue of potential conflict or conflicting views within NATO, as the US contribution openly and broadly supports that transformation. It is difficult to find reliable written sources, but we discovered a discrepancy in the answers from our local respondents versus KFOR personnel in this question. By KFOR personnel, we were told that KSF, which is known for embracing active UCK leaders from the time of war, openly showed their homage to the UCK in their HQ and that, in reality, there were no longer ethnic Serbs in the force. By the local respondents, there was also a recognition of challenges in diversity, but KSF was not viewed as exclusively Albanian. It is important to stress that we have no impression of 'political answering.' It is likely a question of perception, as the KSF is officially open to all Kosovo citizens. For KFOR, a prominent theme in the PsyOps messaging is interethnic tolerance. The good experiences from the Kosovo Police are used as a stepping-stone to broaden that perspective.

Figure 3-2: The Bridge Over the River Ibar Divides the Two Parts of Mitrovica into an Albanian and Serbian Part. Private photo from Mitrovica in November 2021. Jeanette Serritzlev.

3.4.3 The State of the KFOR Mission

The KFOR mission is neutral in the question of the independence of Kosovo, and it supports local stability without intervening in ethnic or political issues [17]. This neutrality could be used to demonstrate KFOR – in the sense of NATO – as weak and unable to exercise power. However, as KFOR is no threat to local authorities or opposition groups, it is difficult for a Russian and a Serbian part to portray the NATO force as an aggressor undermining the will of the people in Kosovo.

Initially, we expected to find more Russian influence directly about or against NATO's KFOR mission. However, we did not find indicators supporting that, nor did our interview respondents. A hypothesis could be that the current state of NATO's KFOR mission is suitable for most regional actors – including Russia and Serbia. The presence of KFOR in Kosovo secures relative stability, and none of the state actors involved seems to have an interest in the opposite. The current situation provides all actors with a wide room for maneuver to pursue their different interests and objectives. Through one informant, we learned that the Russian narrative was more focused on the US presence in Kosovo, particularly Camp Bondsteel, and not preoccupied with the KFOR mission. Besides some articles on Sputnik and RT, we have not been able to find concrete news stories supporting that [18].

In this chapter, we have tried briefly to frame the current situation in Kosovo. This informs our understanding as we look further into Russian national interests in the Balkans and in Kosovo specifically and how it is executed.

3.5 RUSSIAN NATIONAL INTEREST IN THE BALKANS AND KOSOVO

Russian interests in the Balkans are a mixture of geopolitical concerns, a long history of shared culture and alliances, and – not to forget – a part of trade and energy policies. In other words, it is vital for the Russian national strategy that the West Balkans are not pushed into the arms of NATO and the EU. As part of the ongoing strategic competition between Russia, China, and the US, Russia must preserve a presence in Southeastern Europe.

The Russian Orthodox Church has very close ties with the Serbian Orthodox Church. Other cultural elements, such as language and ethnicity, connect Russia to this part of Europe. Promoting an alternative model to the West of a "Russian civilization" will have a fair chance here [19] p. 9. Russia's loss of power due to the collapse of the Soviet Union and the dissolution of the Warsaw pact has had a tremendous impact on Russian self-understanding and approach to international politics. The current NATO-Russia crisis relating to Ukraine at the time of the report is an obvious example of this.

Russia has witnessed its power structures and spheres of interest diminish; it also saw the Baltic states and the countries of the former Warsaw pact enter Western alliances such as NATO and the EU. Currently, Russia is determined to keep some influence in the Caucasus, Central Asia, and Ukraine.

In the Balkans, Russian influence and power are also diminishing rapidly. In 2017, Montenegro became a NATO member, and in 2020, North Macedonia joined the alliance. Even Russia's closest ally in the region, Serbia is a partner of NATO; the same goes for Bosnia-Herzegovina. The situation is similar when it comes to the EU. The entire West Balkan region negotiates for closer relations or even union membership. The countries are potential candidates or have association talks with the EU. These talks include Kosovo despite the lack of recognition of statehood from all EU member states. This institutionalization toward a western order and western priorities pushes Russia out of the European continent. So what can Russia do to push back and stop these developments in the making? Not much. It lacks the economic muscles to buy influence and commitment to a Russian-led alternative. It lacks allies and friends who will follow and depend on Russia of their choosing. It lacks means of coercion as well as soft power. When we met in Pristina, Florian Qehaja from KSCC addressed Russia's options this way: *"Russia doesn't have much to offer. Its best option is to be a spoiler at the macro-level"* [20].

Russia's best chance for spoiling in the Balkans is to gain a regional foothold through Serbia. A recent KCSS report concluded that "Kosovo is the bargaining chip *Russia uses to get what they want from Serbia. Russia needs a friendly base of operation in the Balkans, and no country is better positioned to do this than Serbia. In return, Serbia relies on Russia's diplomatic capabilities to promote and protect its claims over Kosovo"* [19] p.11.

What can Serbia offer in return for Russian support of Serb minorities and former territorial issues? Serbia has allowed Russia to control the Serbian oil and gas sector, and Serbia imports 65 – 70 % of all its gas and oil from Russia. Serbia has supported Russia and not imposed sanctions on Russia for its annexation of Crimea, as both nations view Crimea and Kosovo respectively as historically and legitimate home territories. Serbia also hosts the Russian Serbian Humanitarian Center in Nis in Serbia. The Russian-Serbian co-founded center was established in 2012, focusing on humanitarian response, natural disaster relief, and man-made accidents [21]. Different sources claim this is a front organization for a Russian intelligence outpost and a base for operations. The location provides Russia with a physical presence in the heart of the Balkans, only 100 miles from the US military base Camp Bondsteel in Kosovo and close to all important destinations in the area' [22], p.13. Fairly to say, similar claims are made about Camp Bondsteel from a Russian/Serbian point of view.

Serbia has had a defence cooperation agreement with Russia since 2013, enabling soldiers from the two countries to train together regularly. Russia has donated six MiG-29 fighter jets, thirty T-72 tanks, and thirty BRDM-2 armored reconnaissance vehicles. A range of maintenance and service contracts attached to the transfer of additional MiG29 and MI-17/35 helicopters have been signed to benefit Serbia and Russia [23], pp. 14-15. . Serbia is divided between different interests from the West, Russia, and China. Serbia has an Individual Partnership Agreement with NATO and has contributed to several EU missions.

Moreover, Serbia has built ties with China regarding investments and loans in the Serbian national security sector, energy sector, and help during Covid. There have also been cultural exchanges and institutionalized cooperation, e.g., inviting Serbia to join the Belt and Road Initiative. Belgrade hosts one of Europe's most prominent Chinese cultural centers [24] p.12.

Consequently, during the last five years, Russia has had to make more significant efforts to convince Serbia that Russia is its closest ally and partner. Suppose Serbia holds the key to Russia's presence in the region. In that case, Russia must use all channels of influence to preserve its special relationship and support the narrative of a strong, long-lasting Slavic brotherhood. This entails fighting for Serbian interest in Kosovo and towards Serb minorities. Russia can achieve this by different means. One way is by promoting the idea of a Serbian World similar to what Russia has done regarding Russian minorities outside Russia. Regarding Kosovo, this means that Russian interests *in* Kosovo will primarily mirror those of Serbia.

3.6 HOW RUSSIA IS ENHANCING ITS INTERESTS REGARDING KOSOVO

3.6.1 Diplomacy and International Organizations

It is relatively easy to pinpoint the overall strategy when looking at Russia's diplomatic approach to Kosovo. Russia argues that Kosovo is a part of Serbia in every possible international forum and must remain so until a settlement satisfactory to Serbia is found. Keeping the status quo for the status of Kosovo is essential. What if Belgrade were to agree with Pristina regarding the status of Kosovo? In that case, Serbia could gain a lot on the international scene; substantial economic investments and trading partners, becoming part of the Western alliance, getting more US funding, etc. On the other hand, Russia would have lost its foothold in the Balkans altogether, not counting Bosnia-Herzegovina. Russia must keep the dispute between Kosovo and Serbia unresolved [25] p. 3.

Since 2010, the UN General Assembly has mandated the EU to facilitate the Kosovo-Serbia dispute. As a result, Russia was left out of the negotiating table [25] p. 9. Still, the Russian diplomats did not have to worry much, with five countries within the EU against the independence of Kosovo; others would safeguard Russian interests within that forum. Just as the Russian diplomats expected, the dialogue facilitated by the EU has turned out to be endless and with no solution in sight. However, from around 2017 to the summer of 2020, a more pragmatic approach from Serbia and Kosovo surfaced. Despite recommendations from the international community not to approach this strategy, a land swap compromise was pushed by Serbian President Aleksandar Vučić and his Kosovo counterpart, Hashim Thaci [23] p.14. If the parties would find a solution to the Kosovo question, how would Russia be able to remain an essential ally for Serbia? In the meantime, Serbia lost its appetite for a land swap once again. This was good news for Russia and many other international players, including the EU, who feared that this could spark new conflicts over the West Balkans.

Faced with enhanced difficulties in preserving its influence in the Western Balkans, Russia has substantially improved its diplomatic relations with Serbia in the last five years. Russia has participated in a lobbying campaign against Kosovo's recognition targeting both countries that have already recognized Kosovo to withdraw their recognition and those countries that have not yet recognized Kosovo, urging them not to do so. In addition, Russia has used its diplomacy to prevent Kosovo from joining international organizations such as UNESCO [26] p.50. In 2018, Russia succeeded in convincing Suriname, the smallest country in South America with around half a million inhabitants, to withdraw its recognition of Kosovo as an independent state. This happened just ahead of the first visit from the Suriname Foreign minister to Russia and a planned visit to Suriname by a Russian business delegation. Until now, more than ten states have derecognized Kosovo's statehood due to the successful diplomatic efforts of Serbia and Russia [25] pp. 4-11. Russia has also used its position to delegitimize policies in Kosovo increasingly in the international community. Through political statements on several occasions, Russia portrays Kosovo as violent towards the Serbian minorities, blames the US for turning KFOR into a US base, and the West for not respecting international law [25] p.17.

Russia's most vital power position at the diplomatic level is its status as a permanent member of the UN Security Council. According to resolution 1244, Russia has continuously argued that Kosovo is an autonomous province of Serbia. For more than a decade, Russia's standpoint remains that it will only accept

an agreement acceptable to Serbia. Russia refuses to set a deadline for the end of talks regarding a Kosovo settlement, turning negotiations into a never-ending story [25] p.15. As negotiations between Serbia and Kosovo became more pragmatic in 2018 and a final solution to the Kosovo question came near, Russia decided to change its position on how a solution could come about. It was no longer only a matter of acceptance from Belgrade. During Putin's visit to Belgrade on January 17, 2019, he restated the position of Russia: Russia favors an agreement between the two parties but adds that it must be confirmed by the UN Security Council, thus giving Russia veto power over the result. Russia will presumably try to block any alteration to the UN Security Council resolution 1244 to keep the situation unsolved. The Russian position on the role of the Security Council regarding a settlement for Kosovo has been repeated several times since then (KCSS, 2020:12). The year 2019 became one of the most intense in relations, visits, and talks between Serbia and Russia, reflecting a rise of importance of Serbia as part of the strategic competition between Russia, China, and the US. Due to COVID, bilateral visits have decreased in the last two years. Still, Russia has stayed on track with its continuous information operations towards Kosovo through diplomacy and more covert through the media, churches, and elsewhere [25] pp. 22-27.

3.6.2 Promoting and Preserving the Serbian World

An indirect approach to Russian influence on Kosovo is to tap into the idea of Russia's cultural, historical, and spiritual relationship with Serbia and the Serbs. Serbia and Russia share the same destiny having parts of their "former citizens" living in other entities. Russia has coped with this with many strategies, including establishing the Russkiy Mir (translated: Russian World) Foundation, which promotes patriotism towards Russia through different sponsored activities in countries that "host" Russian-speaking citizens [27]. To some extent, Serbia has copied this concept. However, the idea of a Serbian World is not an official Serbian policy. Still, there are many examples of vocal support from the government for the idea of a Serbian World and political and cultural initiatives that connect Serbs outside Serbia closer to the motherland [28]. These initiatives focus mainly on a more extensive Serbian influence in Montenegro and Republika Srpska, but they can also have significant implications for Kosovo.

The concept of the Serbian World combines the perseverance of cultural heritage among Serbs in and outside the Serbian territory with an ambition that Belgrade should decide on every issue of vital importance concerning Serbs wherever they live. A range of documents from the government supports this ambition as a legally founded policy toward Serbs in the region [29] p.4. One of those initiatives is the Law on Citizenship for persons of Serbian ethnicity who live outside the Republic of Serbia. Serbian citizenship is obtained easily without renouncing the other citizenship simply by signing a statement identifying oneself as a Serbian. Moreover, the Serbian World concept has a dominant narrative that underscores the vulnerability of the Serb communities. The diaspora needs protection from the Serbian state, and Serbia will not abandon this commitment [29] p.3.

Another recent and illustrative example of how the Serbian World idea connects Russia, Serbia, and the Serb community in the Balkans is the erection of the statue of Stefan Nemanja. Stefan Nemanja is one of the founding figures of Serbia, born in what is today Montenegro, a Serbian prince, monk, and saint. This figure connects the Serb ethnicity's politics, religion, history, and culture. Moreover, the erection is illustrative of how the identity of Serbs is persistently understood through the prisms of heroism, suffering, and armed warfighting [30] – another characteristic corresponding with how Russia views its national fate and cultural heritage. The ceremony in 2021 provided an event to reunite an international network. It was attended by critical persons religious and political from inside and outside Serbia, including Russia. They included the President of the Republic of Serbia Aleksandar Vučić, Chairman of the Presidency of Bosnia and Herzegovina Milorad Dodik, Mayor of Banja Luka Drasko Stanivukovic, Member of the Parliament of Montenegro, and President of the Democratic People's Party Milan Knezevic, President of the New Serbian Democracy Andrija Mandic, Member of the Assembly of the Republic of Northern Macedonia, and President of the Democratic Party of Serbs in Macedonia Ivan Stoilkovic, Bishop Jovan of Šumadija, Bishop Irinej of Bačka, Bishop David of Kruševac, Vicar of the Temple of St. Sava, Vicar Bishop of Remezija Stefan, Vicar Bishop of Mohács

Hesychius, and importantly, the Ambassador of the Russian Federation Alexander Bocan-Kharchenko [31]. On the official website of the Serbian Ministry of Defense, an article in the summer of 2020 explains the symbolic value of the statue's placement; *"That Belgrade becomes what it should and must be – the capital for all Serbs"* [32]. The concept of a Serbian World is one of the tools to engage and mobilize the Serbian community culturally and spiritually. It is useable politically because of its soft power potential as a Russian-led alternative to the West. Besides promoting the Serbian World concept, Russia has chosen other affordable means to secure its relevance and presence in the Balkans.

On the one hand, as the last chapter pointed out, Russia invests in direct diplomatic firmness in international institutions, including exploiting its unique position as a permanent member of the UN Security Council. On the other hand, Russia engages more covertly in continuous information operations regarding the lack of legitimacy of Kosovo's independence and governance. The information operations work towards the Serbian community in Serbia and Serbian minorities, and different audiences of relevance around the world [25] p. 24.

3.7 THE ORTHODOX CHURCH

In most countries where the Orthodox Church plays a substantial role, there are close ties between the state, Church and the national identity [33]. Serbia is no exception. In Serbia, ethnicity and religious identity almost have identical meanings. This provides the Serbian Orthodox Church with a joined political and cultural role acting as a media for Serbian (and Russian) soft power in the Serb communities within and outside the Serbian state. The close ties between the political Belonging to the Serbian Orthodox church imply that you are Serbian, part of the Orthodox cultural unity, and therefore also have Belgrade as the main point of reference regardless of your country. This core element of Serbian identity also means that it is hard to distinguish the concept of the 'Serbian World' from the Serbian Orthodox Church. Likewise, separating the Russian Orthodox Church (ROC) from the Serbian Orthodox Church (SOC) is difficult. The two churches have a strong connection and are closely related to each country's political system.[3] Russian influence through the SOC is to be taken seriously [7], p. 29, including both *on* and *in* Kosovo.

In 2018, Patriarch Irinej from the Serbian Orthodox Church led a delegation to Moscow. At this event, he stressed that the spiritual center for all Orthodoxy is the Russian Orthodox Church. He declared that Serbs would always look to Russia for assistance and be the small boat tied to the great Russian ship. This speaks directly to the Russian national interest of becoming an alternative to Western culture and values. Patriarch Irinej also addressed similarities in experiences of the Churches in Russia and Serbia. He stressed that outside today's Serbia, Slavic ancestors shed blood defending their Christian faith at the Kosovo Polje. This reference to 1389 underscores why Serbia must not give up on this territory. The same goes for Ukraine, the core of the Kievan Rus Empire, and Kyiv as the mother of all Russian cities. The Patriarch spoke to merging high politics and spirituality, uniting powerful elites' agendas, and the people's longings for a more glorious past [34] p.69. That is essential, what the Serbian World concept is about, and why this has great potential for Russian strategies in the Balkans.

The Russian Orthodox Patriarch Kirill is a vital voice with solid ties to the Kremlin. He has publicly spoken about the Serb minorities and the Serbian Orthodox sanctities in Kosovo. Kirill has also emphasized supporting Kosovo Serbs and sanctities by funding the restoration of churches [35] p. 116. Several of our respondents stated that Albanian identity is founded on ethnicity and language, where religion is considered private. The Serbian identity, on the contrary, cannot be separated from the Orthodox Church. That does not necessarily mean that every Serb is religious. Significantly, however, the relationship between individual identity and the national strategic culture is based on the values and traditions of the Church. From a Russian viewpoint, the SOC becomes a powerful tool that can parallel or separate from the political level. E.g., the Russian Patriarch Kirill, in a meeting in 2015 with the Serbian Minister of Justice, expressed his concern

[3] For an examination of the two churches, see Srdjan Barisic, "The Role of the Serbian and Russian Orthodox Churches in Shaping Governmental Policies" [35].

over Montenegro approaching NATO membership [35] p. 119. In this way, when the Serbian government shows a more open attitude toward NATO or the EU to obtain benefits or enter into agreements, the SOC simultaneously can be influenced or used as an agent of influence to maintain skepticism on both NATO and the EU within the Serbian community.

3.7.1 Russian Information Operations in Media Outlets: Sputnik Serbia and RT

According to our initial research, we had expected to find more direct influence activities in Kosovo and regarding Kosovo internationally. We found less focus on Kovoso specifically but more on the region in general and on Kosovo whenever it is beneficial. In the case of the independence question, Russia supports Serbia as a close partner nation; however, also by framing the similarity between Crimea and Kosovo. Interestingly, even though the cases are different, the framing of the "Crimea is Russia – Kosovo is Serbia" seems– at least to some extent – to be perceived relatively successful among some audiences (Figure 3-3).

Russia is not the only state actor with interests in the Balkan region. However, according to a study from the European Parliament, Russia is by far the only actor with such a broad spectrum of influence activities in the region compared to China and Turkey. In the case of China and Turkey, influence activities are typically case-oriented. In contrast, themes portrayed by Russia are much broader in scope, intending to shape perceptions in a wide range of areas [36] pp. 34-35.

Figure 3-3: Comparison Between Crimea and Kosovo. Private photo from Mitrovica in November 2021. Jeanette Serritzlev.

Supporting our findings, a study requested by the European Parliament in 2021 states that Kosovo differs from other Balkan states: *"Kosovar politics and media – and, as a result, Kosovo's disinformation landscape – are peculiarly international."* [36] p. 25. In addition, the report concludes, the levels of disinformation, with issues related to the pandemic as a deviation, including influence from Russia, Turkey, and China, were lower in Kosovo than in most parts of the Balkan region [36] p. 26. In conducting research on Russian influence operations, we did not find significant information or indication of media activities directly targeting the KFOR mission. KFOR is mainly addressed in news

outlets such as Sputnik Serbia.[4] When asking interviewees about Russian influence activities, there seem to be different views: That it is strong but difficult to point out, or that it is integrated with the Serbian activities, and that it should be seen more as Russian support to Serbia. It is a shared understanding among our respondents that Sputnik Serbia is the main platform for distributing pro-Russian narratives regarding Kosovo (our interview respondents; [6] p.10). This is also the conclusion of a report made by KIPRED in 2021. The executive director of KIPRED, Lulzim Peci, with whom we met, called it a *"Russian diplomatic war against Kosovo*" [37]. According to an analysis from the NATO StratCom CoE from 2020, the overall narratives portrayed in Sputnik Serbia are as follows [38], p. 48.

Defining Narrative	Number of Articles
The WB region is unstable, and there is a high potential for conflict	765
The WB region is a playground for the clash of interests between East and West	576
Human rights are under threat	174
The EU is hegemonic	128
WB countries are weak and incapable/corrupt	106
NATO is aggressive and provocative	57

The 'NATO as an aggressor' narrative is the lowest according to the number of articles, but it is still worth noticing. According to the report from the NATO StratCom CoE, the sub-narratives about NATO focus on two issues:

1) NATO's support to creating a Kosovarian Army.
2) NATO's use of depleted uranium during the bombings in Kosovo and Bosnia.[5]

It is interesting to notice that the subnarratives do not focus on the KFOR mission of today but on the support to KFS in another NATO or US configuration than KFOR – and on actions made during the war. It indicates that Russia see no advantage to be gained be characterizing the KFOR mission of today as a problem. In the main English version of RT (rt.com), several articles on Kosovo exist. One article dated October 23, 2021, is about two Russian diplomats to UNMIK being expelled, allegedly due to malign influence: "*Kosovo's de-facto government is illegitimate, and the expelling of two Russian diplomats on UN business has no legal force*" [42] The article is an 'RT classic' denying the justification of Kosovo as a state and hence the following not able to expel foreign diplomats. Also, as common, the article ends by summarizing NATO actions in 1999 as a pro-Albanian intervention. Other Kosovo-related articles on RT's webpage in general focus on undermining the authority and neutrality of public institutions in Kosovo [43], [44], ethnic tension [45], and the idea of creating a Greater Albania [46], caused by a recent statement of the Albanian Prime Minister Edi Rama in an interview in October 2021 [47]. Serbia and Serbian communities in other Balkan countries are by the NATO StratCom CoE named the 'Serbosphere,' which includes Republika Srpska in Bosnia-Herzegovina, Montenegro, the Serbian population in Kosovo, and to a certain degree North Macedonia (NATO Strategic Communications Centre of Excellence [38], p.24. In the 'Serbosphere,' the narratives are in general pro-Russian. The theme of Slavic brotherhood is widely used [38], p.24. According to the NATO StratCom CoE report, the pro-Russian influence is not limited to Russian-controlled media such as Sputnik Serbia, but on the contrary, primarily based on local Serbian media, that being state-controlled or private media outlets. (NATO Strategic Communications Centre of Excellence [38], p.25.

[4] See, for example, this article from November 8th 2021: "KFOR Assessed the Situation and Revealed What is Crucial so that the Situation in Kosovo and Metohija Would Not Escalate" [39].

[5] For NATO's own public information about the depleted uranium see Ref. [40]. Also see transcription from a NATO press conference on the topic in 2001 [41].

To conclude, there seems to be relatively little directly anti-KFOR influence activity. Those focusing on Western military presence in the Balkans talk about NATO as a whole or the US presence specifically. Also, the Balkan wars in the 1990s are used as a line of messaging. This analysis of the Russian media outlets supports our other findings indicating that Kosovo, in many ways, is more a *subject of influence* rather than a *target of influence.* This is ***not*** a conclusion of foreign influence not being a concern for the Kosovo authorities, but that it seems more to be a concern of international politics than an internal one.

3.8 KFOR'S RESPONSE TO RUSSIAN INFLUENCE ACTIVITIES

As KFOR was the main subject of our research, we expected to look into how KFOR responded to different kinds of influence activities. Meantime, we have learned that KFOR does not do much to mitigate or counter Russian activities, as these scattered and low-key activities do not constitute a direct threat or challenge to the mission. That supports our general findings of Kosovo's role in the region: We argue that KFOR plays a part in a more significant narrative battle about NATO, but the KFOR mission does not seem to have any significant interest from it the Russian side.

Accordingly, from the Serbian perspective, Belgrade keeps a skepticism towards NATO in general and maintains the memory of the NATO 1999 bombings of the capital. However, even in the Serbian enclaves in Kosovo, KFOR does not seem to be perceived as taking sides regarding the future settlement in Kosovo. On the contrary, both locals and KFOR respondents believe that KFOR broadly is viewed as a guarantee for security and stability for the Serbian as well as the Albanian communities within Kosovo. One could argue that KFOR's response to internal and external critique mainly takes the shape of Posture Presence Profile (PPP) measures, cultural awareness, and all other kinds of actions of inclusion for all parties. As we were invited on an atmospheric patrol with the Danish Tactical PsyOps Team, they paid great attention to these issues, including how to act and pose—not staying too long in 'disputed areas,' being either UCK memorials or Serbian places of worship.

3.9 CONCLUSIONS

Even though we could not detect explicitly Russian influence activities *in* Kosovo to the extent we had expected, the report shows that Russia is hugely influential regarding the fate of Kosovo. Viewed from a regional lens, Kosovo remains one of the critical pieces of a larger puzzle of Russian influence in the Balkan region. Following this line of reasoning, it is essential to distinguish between Russian influence activities *in* Kosovo and *on* Kosovo. Russia is deeply interested in non-recognition by the world community of Kosovo as an independent state. Importantly, however, this interest stems not from any concerns regarding Kosovo itself, but from Russia's vital interest in supporting Serbia's agenda. Through direct cooperation with the Serbian political leadership on shared national interests, Russia keeps a foothold in this region. A foothold which Russia risks losing, if the process of NATO and EU expansion continues. Russia would not invest its diplomatic power position in Kosovo's future settlement if this did not tie Serbia to Russia. However, keeping Serbia as a close ally is a national objective, and it does not come as easy as it used to in the past. Serbia, with the current political leadership, has willingly cooperated with China, the EU, and NATO in order to attract means or money. The Serbian president Aleksandar Vučić is known for his balancing strategy between Russia and the West.

In recognition of this, Russia also engages in more indirect means of influence towards ethnic Serbs throughout the Balkan region, supporting activities in the Serbian world community through different societal groups, media, and, not least, the Orthodox Church. All initiatives to keep Serbia in line with Russian objectives. The overall support from Russia and Belgrade's importance for all Serbs leaves Serbian political leadership with little room to deviate from Russian priorities.

As part of our problem statement, we wanted to look at how KFOR responds to different Russian influence activities in Kosovo. However, KFOR has not put much effort into this, mainly because Russian activities are not a severe challenge to the KFOR mission. Before conducting our research, we expected that KFOR did not deter Russia and Serbia from taking additional steps to destabilize Kosovo. However, this report has provided a regional lens to evaluate KFOR's activities in Kosovo. By mandate, KFOR does not take sides regarding the question of independence, and local Serbs and Kosovo Albanians perceive KFOR as helpful in supporting security and stability in Kosovo. As long as KFOR does not change this neutral position, the mission seems to satisfy most actors, including Russia and Serbia. In that respect, one can claim that KFOR successfully mitigates Russian influence on ethnic groups in and around Kosovo. From the regional perspective, KFOR's low-key approach, staying well within the mandate of UN resolution 1244, has given NATO a unique position to provide the citizens of Kosovo with stable conditions. The stability and security provided by NATO have made the foundation for societal development and economic growth, created in cooperation with e.g., EU. KFOR has by large done this for a long time without positioning itself as a direct target for criticism or discord from Russia, Serbia, or other actors.

This is a great achievement for KFOR and NATO; however, the status of Kosovo is still not clarified, and the political challenges are unsolved and linger. This allows Russia's influence operations, together with other political and diplomatic means, to continue pushing Serbia towards a confrontational position towards Kosovo and throughout the region. This political stalemate is for the EU and US to try and solve.

3.10 CONSIDERATIONS FOR NATO IN LIGHT OF THE UKRAINE WAR

1) The current state of Russian-Western relations, which most likely will last for long, might encourage Russia to increase its efforts in the Balkan region in order to deter or disrupt a deeper integration into EU and/or NATO.

2) NATO must expect Russia to use relevant resources to stay in the Balkan region, including Montenegro, Serbia, and Bosnia influencing the Serbian world.

3) Russia may lack diplomatic power in the West; it has, however, gained a new role for states in Africa and South America that can prove helpful in the UN system—helping to unsolve growing ethnic conflicts in the Balkan region, including Kosovo.

4) Russia may rely on proxy agents, e.g., the Orthodox Church, for much of its activities in the Serbian world supplementing Russia's influence through official means and activities.

5) As Serbs experience exclusion from Western connections due to the war in Ukraine and the Serbian unwillingness to support Ukraine continues, there is a risk of a spillover effect, which potentially could lead to increased destabilization in Serbia, Bosnia, Montenegro, and Kosovo. The Russian and Chinese influence may grow as a result of this.

6) The relative stability in Kosovo may be jeopardized to some extent if the Serb minority feels more alienated and the Kosovo political leadership is tempted to take further steps at statehood, e.g., through KSF developments in light of a weakened Russia.

7) As the Balkan region is a affecting the security situation in all of Europe, it is vital for NATO, as well as the EU, to maintain and potentially strengthen situational awareness in all of the region.

8) Overall it seems less likely that Russia in the near future will have the will or resources to considerably increase its activities toward Kosovo. Moreover, even if an increase in influence activities *in* or *on* Kosovo occurs, the mere presence of KFOR seems to remain the best guarantee for peaceful developments in Kosovo.

3.11 REFERENCES

[1] Fitzpatrick, M. "Sowing Discord, Countering Fear: Force Protection and Resilience to Disinformation." DRDC– Centre for Operational Research and Analysis, International Command and Control Research and Technology Symposium, Southampton UK: November 2020.

[2] Fire Eye Report. "Ghostwriter Influence." Mandiant, 21 February, 2020.

[3] World Population Review, "Countries that Recognize Kosovo." https://worldpopulationreview.com/country-rankings/countries-that-recognize-kosovo Accessed 01 November 2023.

[4] European Parliament, "VP/HR – Withdrawal of Recognition of Kosovo." Question for written answer E-006438-18 to the Commission (Vice-President/High Representative), Rule 130, Dominique Bilde (ENF), 20 December 2018. https://www.europarl.europa.eu/doceo/document/E-8-2018-006438_EN.html

[5] KoSSev, "Dacic: Sierra Leone 18th State to Withdraw Kosovo's Recognition; Pristina: We Have Nothing to Confirm." Kosovo Sever Portal, 3 March 2020. https://Kossev.Info/Dacic-Sierra-Leone-18th-State-To-Withdraw-Kosovos-Recognition-Pristina-Denies/

[6] National Democratic Institute (NDI). Kosovo: Post-Election Analysis of February 2021 Parliamentary Elections, 2021.

[7] Kosovar Centre for Security Studies (KCSS). "Russian Interference In Kosovo: How and Why?" 2017.

[8] Zivanovic, M. "Russia Backs Serb Party Joining Kosovo Govt." BalkanInsight, 14 September 2017. https://balkaninsight.com/2017/09/14/putin-s-united-russia-supports-kosovo-serb-party-09-14-2017/

[9] Begisholli, B. "Serbian-Funded Kosovo Housing Estate Sparks Political Row." BalkanInsight, 27 March 2019. https://balkaninsight.com/2019/03/27/serbian-funded-kosovo-housing-estate-sparks-political-row/

[10] Radonjic, M. Homecoming Kosovo Serbs Face an Uncertain Future. BalkanInsight, 14 December 2017. https://balkaninsight.com/2017/12/14/homecoming-kosovo-serbs-face-an-uncertain-future-12-11-2017/

[11] BalkanInsight, "Kosovo Serbs Say Belgrade Not Paying Wages." BalkanInsight, 1 April 2008. https://balkaninsight.com/2008/04/01/kosovo-serbs-say-belgrade-not-paying-wages/

[12] Baliu, D. "Kosovo Spends €2.5 Million Paying Non-Working Serb Employees." BalkanInsight, 27 October 2020. https://balkaninsight.com/2020/10/27/kosovo-spends-e2-5-million-paying-non-working-serb-employees/

[13] Balkan Policy Research Group, Public Companies in the Northern Kosovo Municipalities: Stuck in Status Quo, Policy Paper, 9 December 2016.

[14] Butcher, J., and Boffey, D. "Tensions Rise at Kosovo Border as Number Plate Row Escalates." The Guardian, 2 October 2021. https://www.theguardian.com/world/2021/oct/02/tensions-rise-at-kosovo-serbia-border-as-number-plate-rowescalates

[15] KoSSev, "Citizens Have Until Friday to Obtain License Plate Stickers, but they Cannot Do So in N. Mitrovica." Kosovo Sever Portal, 5 October 2021. https://kossev.info/citizens-have-until-friday-to-obtain-license-plate-stickers-but-they-cannot-do-so-in-n-mitrovica/

[16] NALT. https://www.nato.int/cps/en/natohq/topics_48818.htm Accessed 01 November 2023.

[17] North Atlantic Treaty Organization. "NATO's Role in Kosovo." 13 October 2023. https://www.nato.int/cps/en/natohq/topics_48818.htm

[18] Sputnik News International "Camp Bondsteel Serbia Kosovo Military Camp." 28 March 2016. https://sputniknews.com/20160328/camp-bondsteel-serbia-kosovo-military-camp-1037105115.html

[19] Kosovar Centre for Security Studies (KCSS). "Russian Influence In Kosovo – In the Shadows of Myth and Reality." 7 November 2020.

[20] Interview with Florian Qehaja, 18 November 2021.

[21] Russian-Serbian Humanitarian Center. https://www.ihc.rs/en/ Accessed 01 November 2023.

[22] Vllasi, E. "Russian Influence in Kosovo – in the Shadows of Myth and Reality." Report 07, Kosovar Centre for Security Studies (KCSS), November 2020.

[23] Bechev, D. "Russia's Strategic Interests and Tools of Influence in the Western Balkans." NATO Strategic Communications Center of Excellence, 11 December 2019. https://stratcomcoe.org/cuploads/pfiles/russias_strategic_interests_in_balkans_11dec.pdf

[24] Prelec, T. " 'Our Brothers,' 'Our Saviours'. The Importance of Chinese Investment for the Serbian Government's Narrative of an Economic Rebound." Policy Paper, Prague Security Studies, 2020.

[25] Kosovar Institute for Policy Research and Development (KIPRED). "Russia's Information Warfare Towards Kosovo: Political Background and Manifestation." Special Policy Brief October 2020.

[26] Qehaja, F. "Acting Against the Normalization: Serbia's Diplomatic Offensive on Kosovo." In D. Philips and L. Peci (Eds.), Threats and Challenges to Kosovo's Sovereignty. NY: Columbia University Press, 2018.

[27] Pieper, M. "Russkiy Mir: The Geopolitics of Russian Compatriots Abroad." Geopolitics, 25(3), 2020.

[28] Dordevic, N. "Serbian World – a Dangerous Idea?" Emerging Europe, 27 July, 2021.

[29] Digital Forensic Center, "The Serbian World – Originally Borrowed Concept – DFC analysis of the Attempt to Merge Montenegro into the Serbian World." Podgorica, April 2021.

[30] Dureinovic, J. "The Monument to Stefan Nemanja in the Context of the Memory of the 1990s Wars." Heinrich Böll Stiftung, 2021.

[31] Government of the Republic of Serbia, "Monument to Stefan Nemanja Unveiled." 27 January 2021. https://www.srbija.gov.rs/vest/en/166853/monument-to-stefan-nemanja-unveiled.php

[32] Ministry of Defence Republic of Serbia, "Minister Vulin: Belgrade Becomes What it Must and Should Be – A Capital of All the Serbs." 28 August 2020. https://www.mod.gov.rs/eng/16389/ministar-vulin-beograd-postaje-ono-sto-mora-i-treba-da-bude-prestonomesto-svih-srba-16389

[33] Roudometof, V. Church, State, and Political Culture in Orthodox Christianity. Oxford University Press, 25 February, 2019.

[34] Baskin, M. "Unpacking Russia's Balkan Baggage." In D.L. Philips and L. Peci, Lulzim (eds.), Threats and Challenges to Kosovo's Sovereignty, Columbia University, 2018.

[35] Ft 17 Barisic, S., "The Role of the Serbian and Russian Orthodox Churches in Shaping Governmental Policies." In Biserko, S. (ed.), The Warp of the Serbian Identity. Belgrade: Helsinki Committee for Human Rights in Serbia, 2016.

[36] European Parliament. "Mapping Fake News and Disinformation in the Western Balkans and Identifying Ways to Effectively Counter Them." Policy Department for External Relations, European Parliament, 2021.

[37] BalkanInsight, "Kosovo Urged to Start Countering Russian Media Disinformation" BalkanInsight, 07 September 2021. https://balkaninsight.com/2021/09/07/kosovo-urged-to-start-countering-russian-media-disinformation/

[38] NATO StratCom COE. "Russia's Narratives Toward the Western Balkans: Analysis of Sputnik Srbija." 2020.

[39] Sputniknews.com. "KFOR Assessed the Situation and Revealed What is Crucial so that the Situation in Kosovo and Metohija Would Not Escalate." 8 November 2021. https://rs.sputniknews.com/20211108/kfor-ocenio-situaciju-iotkrio-sta-je-kljucno-kako-situacija-na-kosovu-i-metohiji-ne-bi-eskalirala-1131385389.html

[40] NATO, "Depleted Uranium." NATO Topics, Background Information. 17 March 2005. https://www.nato.int/du/home.htm

[41] NATO HQ, "Transcript of Press Conference by Secretary General, Lord Robertson." 10 January 2001. https://www.nato.int/docu/speech/2001/s010110a.htm

[42] RT, "Kosovo's de-facto Government is Illegitimate and its Expulsion of Two Russian Diplomats on UN Business Has No Legal Force — Moscow." 22 October 2021. https://www.rt.com/russia/538234-kosovo-serbia-diplomats-expulsion/

[43] RT World News, "Kosovo's Albanian Police Ban Serbian License Plates, Use Tear Gas Against Protesters, as US and EU Urge 'Restraint' on Both Sides." 20 September 2021. https://www.rt.com/news/535365-kosovo-serbia-roadblocks-standoff/

[44] RT World News, "Serbia's President Blasts World's 'Thunderous Silence' over 'Occupation' of Northern Kosovo as Tensions in Breakaway Region Soar." https://www.rt.com/news/535873-serbian-president-kosovo-tensions/

[45] RT, "10 Albanians Arrested in Kosovo after Attacking Serbs as Ethnic Tensions Flare, Drawing in Serbia & NATO." https://www.rt.com/news/536006-albanians-arrested-northern-kosovo/

[46] RT, "Annexing Kosovo to create 'Greater Albania' would shatter peace in Balkans, Russia warns, telling West to help end 'provocations'." 11 October 2021. https://www.rt.com/russia/537161-annexing-kosovo-balkans-russia/

[47] Euronews, Albania. "Russia reacts to Rama's Greater Albania statement: Encouraging such plans undermines regional stability." https://euronews.al/en/russia-reacts-to-ramas-greater-albania-statement-an-albania-kosovo-unification-undermines-regional-stability/ Accessed 01 November 2023.

Chapter 4 – ANALYSIS OF CURRENT INFORMATIONAL ASPECTS OF PROBABLE SCENARIOS FOR THE DEVELOPMENT OF A MILITARY CONFLICT WITH THE RUSSIAN FEDERATION

Volodymyr Bashynskyi
State Scientific Research Institute of Armament and Military Equipment Testing and Certification
UKRAINE

Hennadii Pievtsov
Ivan Kozhedub Kharkiv National Air Force University in Science
UKRAINE

Pavlo Open'ko
National Defence University of Ukraine
UKRAINE

Anatolii Salii
National Defence University of Ukraine
UKRAINE

4.1 INTRODUCTION

Modern warfare uses integrated political, economic, informational, and other non-combat measures underpinned by threat of military force. The combination of these methods implements the main concept of hybrid warfare. This method means to achieve the political goals through the use of modern information technologies, the cautious application of hard power, and a minimal use of combat power. The peculiarity here is that it is disguised, uses non-linear tactics, and is aimed at obtaining patronage over the state instead of occupation of territory (although it is possible to take control of some separate territories). It can be achieved through the impact on the population, politics, business, and security agencies.

The Russian Federation has readily adopted this concept of warfare and while its recent actions demonstrate a broad-ranging policy of influence targeting Europe, the European Union, the USA, and others, a primary example of all aspects of hybrid warfare is the Russian Federation's actions against Ukraine. It is reasonable to assume that the RF will employ such methods over the coming years.

The purpose of the research covered in this chapter is to determine, based on a scenario-forecasting method, some of the possible variations of the informational aspects of the ongoing military conflict with the Russian Federation out to 2035 as well as to estimate the possibility of large-scale armed aggression against Ukraine based on each variant identified.

To formulate our predictions, scenario analysis tools were used, namely: the identification and analysis of the most influential factors likely to affect regional relations out to 2035. This then allowed for the creation of a basic status quo (or baseline) scenario. The correlation between the conditionally independent main influential factors was then analyzed to build a range of plausible scenarios. It is impossible to predict the future with any accuracy and it is apparent that the scenarios may not occur as described and that, in reality, the main features of several scenarios will be apparent in future events with, perhaps, the main feature of one scenario being predominant.

4.2 SCENARIO DEVELOPMENT CONTEXT

4.2.1 Object and Primary Actors

At its root, the object of the conflict between Ukraine and the RF is the diametrically opposed views on the political, social, and developmental alignment of Ukraine. The main subjects of the conflict in our scenarios are Ukraine, the Russian Federation, the United Nations (UN), European Union (EU), NATO, the primary

individual EU member countries that neighbor Ukraine or are in Eastern Europe, EU member countries that consistently demonstrate a leadership role, and the United States of America. The determination of these conflict subjects is due to the possibility and importance of their impact on the international and regional (European) security, Russian Federation, and Ukrainian policies, and the intersection of their respective interests in conflict development in the region and during the timeframe under consideration.

4.2.2 Conflict to Date

According to UN estimates, the conflict in the East of Ukraine "is one of the deadliest in Europe since World War II." During six years of warfare in Donbas more than 13,000 people have died, approximately 30,000 have been wounded, and about 1.8 million inhabitants of Donbas and Crimea have been internally displaced. 17,000 km^2 of Donetsk and Luhansk territories remain occupied, and, when added to Crimea's area of 27,000 km^2 area, some 7.2% of Ukrainian territory remains occupied by the RF and its proxy forces. 409,700 km of the Ukrainian-Russian border remains uncontrolled. Ukraine has suffered huge financial and economic losses. Thus, 27% of the Donbas industrial potential was illegally transferred to Russia, including the equipment of 33 large industrial concerns located in the region.

4.2.3 Geopolitical Factors

Simultaneous to the onset of RF aggression against Ukraine is the increase of geopolitical competition between major powers. This competition has geographic, financial, resource, and political dimensions and has been accompanied by trends indicating wide-spread increases in military spending and a race to develop new weapons systems.

Our research has led us to identify the following major features of the security environment as necessary factors to consider in our scenario development process:

- Intensification of the disagreements on the division of spheres of influence between major powers, characterized by increased aggressiveness, assertiveness, stubbornness, and a desire to alter the military-strategic balance, particularly the escalation of the confrontation between USA and RF;
- Deterioration of security environment in the Middle East and South Africa; the continued problem of religious extremism, including in Central Asia countries, ongoing territorial disputes between Asian-Pacific states over the ownership of the islands;
- Reduced predictability in the international security system; the weakening of the role of international security institutions, attempts to strengthen the role of military force outside the mechanisms of international security;
- The increased use of proxy, irregular, and other informal armed forces in military conflicts contrary to international, the increased emphasis on the integrated use of combat and non-combat instruments (economic, political, informational and psychological, etc.), which fundamentally changes the nature of conflict and warfare;
- Open violation of the norms and principles of international law, written in the UN Charter, the Final Act of the Conference on Security and Cooperation in Europe of 1975 and other international treaties;
- The disregard for legal restrictions on the use of military force by states outside their territory;
- Global climate change, a decrease of the natural resources, shortage of drinking water, food, increased migration, as well as increasing risks of large-scaled natural and man-made disasters; and
- Expansion of terrorism, piracy, other phenomena related to the use of armed violence.

4.2.4 Defined Threats to Ukraine's National Security

The current state of Ukraine's national information infrastructure is insufficient to effectively anticipate, counteract, and respond to the information operations of the aggressor. In addition, policy and legislation gaps, difficulties with sustaining the strategic narrative, and poor social media culture affect Ukraine's ability to operation in the information domain. Combined, these factors limit the ability to protect and further the national interests of Ukraine.

The *Doctrine of the Informational Security of Ukraine* defines the current threats to national interests and national security of Ukraine in the informational sphere remain:[1]

- Special informational operations, aimed at undermining Ukraine's defence capabilities, demoralizing military personnel, provoking extremist behavior, feeding panic, escalating and destabilizing the socio-political and socio-economic situation, and stirring inter-ethnic and inter-religious conflict in Ukraine;
- Special informational operations by the aggressor state outside of Ukraine with the aim of creating a negative image of Ukraine in the world;
- Expanded control or influence of the aggressor state and proxy organizations over information technology infrastructure in Ukraine and occupied territories;
- Complete domination of the information domain by the aggressor state on the temporarily occupied territories;
- Spreading calls for radical actions, propaganda of the isolationist and autonomous concepts of Ukrainian regional coexistence;
- Russia's constant use of special narratives and informational labels ("warfare party," "Kyiv junta," "Banderites," "fascists," "Nazis") by the Russian Foreign Ministry and political levels to delegitimize the Ukrainian government;
- Creation of propaganda channels by Russia that works on discrediting the Ukrainian government on the target groups;
- Open and covert use of the EU democratic norms and procedures, as well as the USA and other partner countries to discredit Ukraine and its attempts to form international support for countering Russian aggression;
- Political and lobbyist measures in the West, used by Russia to build up doubts on the correctness of the EU's position on the continuation of sanctions against the Kremlin, as well as to legitimize the annexation of Crimea;
- Expanded use of the ROC – UOC-MP by Kremlin with the creation of new propaganda and disinformation flows to Ukraine in order to demoralize and disorient the population, reduce its resistance to the aggressor;
- Use of the Ukrainian TV channels and other media to broadcast pro-Russian narratives in dosed form or under opposition slogans;
- The predominant use of Russian social networks by Ukrainian citizens (even despite the ban in Ukraine) for communication and receiving/sharing information;
- Extending of information products by using regional, ethnonational, linguistic, and other identities among the Ukrainians to divide society, impose a sense of discrimination and insecurity, prepare a social base for rebellions and provocations;

[1] An English language translation of the Doctrine is available at https://rm.coe.int/doctrine-of-information-security-of-ukraine-developments-in-member-sta/168073e052 (link current as of April 2022). The formal articulation of informational threats is on p. 2.

- Formation of isolated socio-cultural and informational reality inside the occupied Ukrainian territories, blocking the access to Ukrainian informational content from residents of these territories;
- Efforts meant to undermine the authority of the Ukrainian expert community by using native-Ukrainians to delegitimize the main evidence of Russian aggression.

Thus, the informational aspect of the military conflict with the Russian Federation in this thesis **is considered as a confrontation** within an informational war that, for Russia, is aimed at keeping the Ukrainians within their sphere of influence and fully responsive to Russian Federation strategic ends. Ukraine, of course, continues to pursue the national idea rooted in independence and complete sovereignty, aligns with a European ("Western") system of values, and divorced from Russian imperial ideology.

The sources material employed in this work include the official documents from Russian Federation and Ukraine and medium-term forecasts related to the international security state in 2030-2050 from various analytic centers.

4.3 ANALYSIS

This research was conducted to inform the development of future-oriented scenarios focused on the informational aspects of the conflict with the RF in support of efforts to find ways of peaceful settlement and completion of the military conflict. The scenario variants are based on the analysis of contemporary events and the themes and characteristics of the informational space around Ukraine.

According to Russian analytic centers, the tensions in the international situation (including for Ukraine) will remain for the entire medium term. The main trends in this material are:

- The emersion of new economic and military-political power centers represented by China, India, Brazil, Indonesia, Russia, Mexico, etc.;
- The weakening of the Western local civilization dominance would be soon accompanied by the increase of military and other types of violence in worldwide policy by the West;
- Military force re-emerging as a determining factor in the leadership of Western local civilization and declines in local independence remains as a result of worldwide policy;
- Eurasian military-political integration is considered as a necessary condition for Russia's Eurasian integrity and the development of the Eurasian economic and military-political union; and
- Multipolarity in the future will reduce the number of identity conflicts and confrontations within separate local civilizations. The scale and intensity of clashes between different local civilizations will increase.

These trends, when considered in conjunction with analysis of current RF behaviors and operations, makes it possible to conclude that **Russia considers war as a determining factor in future international relationships. This suggests that Russia's future informational policy and behavior will be extremely aggressive.**

4.3.1 Basic Scenario ("Slow Move")

4.3.1.1 Informational Influence of the Russian Federation on Ukraine

During a significant historical period, Ukraine was a part of Imperial Russia and the USSR. Therefore, the Russian Federation continues to consider it as a part of its geopolitical sphere of influence and denies the legitimacy of an independent Ukraine. Within this context, the primary focus of RF informational influence targeting Ukraine are:

- The informational infrastructure of the state;
- Awareness, will, and feelings of servicemen and different segments of civilians, especially during elections and crisis;
- Management decision-making systems in political, economic, social, scientific, and technical spheres and in the sphere of providing security and defence of the state;
- Critically-placed contingent (opposition, dissidents, criminals, etc.) as means to intensify crises in Ukrainian society;

Simultaneously, the main object of influence in the informational war against Ukraine are civilians, who "is liberating from Ukrainian junta and fascists" to increase mass hysteria and resistance to legitimate government and support the aggressor.

Currently, the democratic development in Ukraine remains unstable and its membership in the Western European political tradition is still in doubt. Therefore, the discrediting of pro-European elites and social destabilization may lead to Ukraine's rejection of the democratic course and, in the long run, to question statehood itself. This window of opportunity is used by the RF primarily for informational influence on Ukraine, supporting the themes of nostalgia for the Soviet Union in the discourse, myths about the specific relationship between Kyiv and Moscow and a mutual history, and the stereotype of Russia as an "older brother," "defender" etc.

In Russian media, the new message gets upstream – "the West has turned away from Ukraine." It forms the opinion that the USA and EU states are indifferent about Ukraine's future, and without Russia's help it will stop existing as a state – politically and economically, eventually, Ukraine must return to Russia voluntarily.

4.3.1.2 Positive Aspects in Counteracting RF Informational Influence

1) Within informational war, Russia actively uses the religious factor. UOC (MP) pursues the goal-oriented and systematic policy of destroying the autocephalous status of the Ukrainian Orthodox Church and, accordingly, the national unity policy in Ukraine.
   - *Ukrainian society's trust in Orthodox churches with Ukrainian direction continues to increase, as well as the support of the UOC autocephalous, which continues to be officially recognized by Constantinople, and is evidenced by increasing the number of parishes.*
2) Expansion of labor migration of Ukrainians to European countries, especially to Poland, and decreasing ones to Russia.
   - *Ukrainian migrants are more fully exposed to Western European information and socio-cultural norms, which, in various ways, reduces direct Russia's informational influence on them.*
3) Increased patriotism of Ukrainians demonstrates the great self-organization of the people. This is one of the few parameters that are marked as improving, signaling greater degrees of national unity.
4) Several positive messages are being formed in Ukraine, directed to the unity of the state: uniting people around the idea of achieving peace.

4.3.1.3 Negative Aspects in Counteracting RF Informational Influence

1) The insufficient ability of the Ukrainian government to conduct strategic communications, which contributes to a low level of understanding of the political agenda among citizens. (Ukraine has some political decisions in this sphere, but extremely insufficient).

2) Lack of unity in the Ukrainian political elite that does not unite even in the face of war, but "drowns" each other on various talk shows. It helps Russia to achieve greater success, than with the help of a weapon, inciting one group of people against another, provoking civil war, and Ukraine does not prevent this.

3) Nowadays a lot of Ukrainian citizens took the aggressor side under the influence of hostile propaganda, supporting or justifying RF actions. Despite the war, almost half of Ukraine has a positive attitude towards Russia, mostly because of the East of the state, but the "brotherly love" to the aggressive neighbor is also distinctive for other state regions. For example, 21% of Ukrainian citizens have a positive attitude towards the Russian government. Positive attitudes towards Russia fell to the 30% level only after Crimea and Donbas but when the active combat actions ended – raised again, and now almost 50% of Ukrainians have a positive attitude towards Russia.

The highest index of the Russian propaganda effectiveness is in the Donetsk region – 50, as well as in Luhansk – 38 (territories controlled by Ukraine). After Donetsk and Luhansk regions, Kharkiv and Odesa regions are prone to support Russian propaganda. In Russia, the population tends to hold negative attitudes regarding Ukraine and there is little evidence of a sense of guilt regarding the RF aggression against Ukraine.

4) Neglect of the language factor of security in Ukraine, weak language policy of the Ukrainian government. The key direction of the Russian informational expansion – language – remains without the proper response from the Ukrainian side. The level of supporting Ukraine's independence is highest among the Ukrainian speakers. At the same time, Russian speakers are almost the only social group, where the support level is significantly less than 50%.

Generally, Russian speakers are 2.5 times more vulnerable to Russian propaganda than Ukrainian speakers. Ukrainian speakers trust the Russian propaganda significantly less because they don't have any reasons to perceive it as "native." This fact explains, why there are no separatists among Ukrainian speakers, and shows that there is a clear correlation between the language spoken by Ukrainians and state security.

5) More influential guides of Kremlin narratives in Ukraine are the national mass media, which are focused, most of all, on transmitting the negative information – "strategy of negativity." Negative information has become a part of virtual reality for many Ukrainians.

The oligarchy nature of the Ukrainian media space creates ideal conditions for Russia's informational influence. Alliances (more or less stable) between business and political groups in Ukraine and Russia allow the Kremlin to influence the editorial policies of national and local media, controlled by these groups.

At the same time, 72% of Ukrainians learn news mostly from Ukrainian TV channels and Internet media (43% only watch TV, 29% also use the Internet). 22% regularly address both Ukrainian and Russian sources of information (9% of them are only TV viewers). Six percent are practically not interested in news from any of the listed media.

6) Social networks are being used actively for informational manipulations, distribution of fakes, the formation of distorted perceptions. The most popular social network in Ukraine is Facebook and that network, as well as YouTube, uses the smart feed. Facebook accumulates posts from all friends' accounts and pages, that a person has subscribed to. Facebook feeds information to users based on perceived interest. Therefore, the informational message, thrown into the network, quickly spreads among a certain group of users. Since 2019, YouTube has been providing countermeasures for hate speech videos, but the vast amount of information that falls on this platform cannot be completely cleared of fakes. The messenger Telegram is the absolute leader in the dissemination of fake information due to the anonymity of publications. Telegram channels have become the primary source of pseudo-insides and informational flows. Entire networks of anonymous channels are now operational.

7) There is almost no broadcasting of Ukrainian TV channels in the Donetsk and Luhansk regions (especially in the occupied portions of those territories) and Russian propaganda carried on Russian-controlled TV channels is effective. There will be a negative tendency to increase the number of people in these territories, who are eager to separate from Ukraine or, at least, to maximum autonomy.

Today, there is a tendency for Russia to increasingly employ low-intensity information measures and to avoid harsh statements in its information campaigns with many of the channels of communication of these "soft power" messages being Russian scientists, artists, religious figures, and others.

There is a general tendency for people to gradually lose confidence in both the Ukrainian (especially in the South and East of the country) and Russian media. People compare the picture on TV with the one they see from the window. If these realities do not coincide, they stop trusting the media.

The basis of non-classical forms of Russia's aggressive policy is the destabilization of the socio-political situation in the country, the use of protest potential of the local population, discrediting in the international arena, the impact on political, economic, energy, social, financial, and other spheres of life. These forms are based on the methods and technologies of information warfare, which Putin, Shoigu, and Gerasimov mentioned in their official speeches and were prescribed in the RF Military Doctrine. To implement their plans, troops and information operations forces were created within the Russian Armed Forces including:

- Information Confrontation HQ in the Operational HQ of the General Staff of the Russian Federation Armed Forces (planning);
- Information Confrontation department within the operational departments of armies and fleets (Armies: 6, 20, 49, 58, 2, 41, 5, 29, 35, 36; Fleets: Baltic, Black Sea, North, Pacific);
- Centers of foreign military information and communication of the General Staff of the Russian Federation Armed Forces (Southern Military District – Rostov-na-Donu, Western Military District – St. Petersburg, Central Military District – Yekaterinburg, Eastern Military District – Khabarovsk), and with the beginning of the annexation of Crimea – the Foreign Military Information Group of the Black Sea Fleet (Sevastopol);
- Departments and centers of information confrontation in military districts; and
- Separate detachments of psychological operations (Performers);

In addition, Russian media are widely involved in information struggle: "Pervyy kanal"; "Russia 1"; "Russia 24"; "RIA Novosti"; RTR Planeta; "Zvezda"; "NTV"; Russia segodnia"; "Argumenty i Fakty"; "Moscovskiy Komsomolets"; "Kommersant"; "RT"; "Sputnik"; Rossiyskaya Gazeta; "VPK" and others. Internet centers have also widely used, the so-called troll factories located in St. Petersburg; Kaliningrad; Belgorod; Riazan; Yekaterinburg; Khabarovsk.

Domestically, RF informational actions abroad are underpinned by domestic propaganda. The topics of anti-Americanism, Euroscepticism, xenophobia, and homophobia are actively used in Russia's domestic informational influence to justify the aggression against Ukraine and the occupation of its territories. The main messages of this portion of Russian propaganda are: The Maidan was organized by the USA, as a result, the nationalists came to power, who threatened Russian-speaking Ukrainians. Crimea was saved, people in Donetsk started a rebellion, and the junta struggles with its citizens, there is a civil war in Ukraine and Russia tries to help the fraternal people.

These outward-looking propaganda themes are underpinned by inward-focused, Russian-positive themes. Russia's leading media create an overwhelmingly positive picture of life in Russia: everything is fine in Russia – there is an effective manager – president here, and there are achievements.

4.3.1.4 Russia's Influence on the European Community

With the help of the media and its agents of influence, Russia convinces the world that Ukraine is guilty of the conflict, violating the rights of Russian speakers, trying to isolate them from Russia, and forcibly drag them into Europe.

Such anti-Ukrainian rhetoric does not infuriate the majority of Westerners, because Russia's messages are not directed against their country. The number of Europeans under the influence of Russian propaganda grows, with many believing that certain Ukrainian regions should be given the right and opportunity to secede, that the government of their quiet and wealthy country should never get involved in Russian-Ukrainian conflict and support sanctions against Russia, sacrificing well-being and exposure to danger.

4.3.1.5 Factors Affecting Scenario Development

The discussion above demonstrates that, for scenario development purposes, the informational aspect of the Russian-Ukrainian military conflict has three primary perceptional lenses: Ukrainian, Russian, and international. It also suggests the major factors that must be considered when designing scenarios meant to inform the evolution of Ukraine's national information policy.

Perceptional Factors:

- The attitude of the world's leading countries to Ukraine;
- The attitude of the world's leading countries to the Russian Federation;
- The attitude (perception of the conflict) of international security organizations to Ukraine;
- The attitude (perception of the conflict) of international security organizations to the Russian Federation;
- The level of presence of Russian (pro-Russian) information sources (media, influential people, political parties, public organizations, etc.) in the world's leading countries information space;
- The level of influence of Russian (pro-Russian) information sources (media, influential people, political parties, public organizations, etc.) on the international security organizations decisions;
- Perception by the world's leading countries of Ukrainian and Russian common history (according to Ukraine or the Russian Federation);
- The level of support the establishment of the Ukrainian Orthodox Church and autocephaly by the world's leading countries (independence from the ROC);
- Protection of the leading countries' information space from Russian cyber-attacks;
- Common history, culture, art between Ukraine and the world's leading countries (e.g., the influence of the Ukrainian diaspora);
- International perceptions of the common history, culture, art between Ukraine and the Russian Federation;
- The presence and activity of the Russian diaspora in the world's leading countries; and
- The presence and activity of the Ukrainian diaspora in the world's leading countries.

Ukraine national information policy influencing factors:

- Formedness of the Russian Federation national idea;
- Formedness of Ukraine's national idea;

- Self-identification level of Ukrainians;
- The Ukrainians' views on the religion issue (support for the establishment of the Ukrainian Orthodox Church and autocephaly);
- The Ukrainians' views on the language issue (the leading status of the Ukrainian language in all Ukrainian regions);
- Living standards in the Russian Federation;
- Living standards in Ukraine;
- The possibility of ethnic conflicts in Ukraine;
- The possibility of ethnic conflicts in the Russian Federation;
- Forces and means that the Russian Federation uses (may involve) in the information campaign against Ukraine;
- Forces and means that Ukraine uses (may involve) to ensure its information struggle and information influence on the Russian Federation;
- The Russian Federation information space safety from information influences;
- Ukraine's information space safety from information influences;
- Presence and activity of pro-Russian forces in Ukraine;
- Presence and activity of pro-Ukrainian forces in the Russian Federation;
- Authority and trust level of the Ukrainians to the state government, state institutions, and both the security and defence sector components;
- Authority and trust level of the Russians to the state government, state institutions, and law enforcement agencies;
- Fatigue of the Ukrainians from the military conflict; and
- Fatigue of the Russians from the conflict.

Taking into consideration these decisive influencing factors, four scenarios can describe the information aspect of the Russian-Ukrainian conflict.

4.3.2 Scenario No. 1: "Independence" (Positive)

Core Elements:

- Ukraine accedes to the EU and NATO.
- Public confidence in the government grows.
- The world's trust in Ukraine grows even more.
- A national idea is formed [reinforced] in Ukrainian society.
- Russia loses the influence on the informational spaces of Ukraine and world leaders.
- The informational space of Ukraine is protected from the Russian Federation's informational influence.
- The military conflict between the Russian Federation and Ukraine ends.

4.3.2.1 Ukraine

There is a comprehension within the country, across all groups and regions, that the conception of "Ukrainians" is legitimated, and that this common identity serves as a response to external and internal threats (the contemporary emergence and reinforcement of the national idea in Ukraine). There is an ability to build trust between Ukrainians, as well as between Ukrainians and other communities. A common dream (vision of the future) is formed, science and education are focused on the future.

Patriots control media and the Internet. It significantly affects the objectivity of informational coverage and the formation of the Ukrainian nation.

Ukraine increases its economic and social value for the world and begins to form its geopolitical subjectivity by applying for regional leadership.

4.3.2.2 Russia

The Russian Federation loses control over Ukraine's informational space and is deprived of the opportunity to influence it. The negative influence of the Russian Federation on the attitude to Ukraine is reduced. The informational influence of Ukraine, Europe, and the world more broadly on Russia's mass media and the Internet increases the dissemination of factual information about European values and human rights within Russia. Russia's economic and political inefficiency increasingly affects its ability to influence geopolitics.

4.3.2.3 Scenario 1: Key Events of 2020 – 2024

In the local elections in October 2020, due to the disappointment of the electorate with the actions of the "Sluha narodu" [Servant of the People (political party)], the representatives of local business elites determine the choice.

The elections to Verkhovna Rada of Ukraine are likely to be won by democratic, pro-Western candidates that would form a coalition majority. With this course of events, we can assume that the political vector of Ukraine's accession to the EU and NATO would not change.

At the same time, the economic downturn caused by the global COVID-19 pandemic, changes in the government due to the conflicts, and instability in the pro-government mono-majority, which had won the 2019 elections to Verkhovna Rada may cause the split and probability of prescheduled parliamentary elections. With such a course of events, it can be considered that a revanchist arrival of pro-Russian oppositional forces is possible, which, in turn, may negatively affect the political vector of Ukraine's development in a variety of ways.

In Ukrainian society, the climate of protest opinion against the whole "government of the past" in 2020 – 2024 turns into an active and conscious discussion of new grounds and principles of suffrage. Dozens of new public figures appear (especially in the regions), who unite in a completely new socio-political movement. This movement is recognized by Western politicians as the most promising for the future political life of Ukraine.

At the request of society, a system of real control mechanisms over the fulfillment of the politicians' promises is formed and introduced, efficiency parameters of the officials' work are created, it has a positive effect on the world community's trust in Ukraine.

The mass media and the Internet pass to pro-Ukrainian owners. The Ukrainian national idea is covered in the informational space to form a united Ukrainian nation.

The trustful information related to the Ukrainian-Russian conflict is increasingly covered in the world's informational space. Russia is recognized as an aggressor state. The support to Ukraine from the world community grows.

The Russian Federation loses control over Ukraine's informational space that will deprive it of the opportunity to influence people's minds. At the same time, the negative influence of the Russian Federation on the world's attitude towards Ukraine decreases.

Possibly, the new powerful sanctions against the Russian Federation would be imposed.

Russia's informational space is covered with trustful information about the Russian-Ukrainian conflict, the real situation in Russia itself regarding human rights and freedoms.

Ukraine may join the NATO block and protect itself from Russian aggression.

The process of the resocialization of Ukrainian temporarily occupied territories begins.

Pro-Russian forces on the Ukrainian territory are likely to intensify the call for prescheduled and multiple parliamentary elections. But the elections are held on time.

4.3.2.4 Scenario 1: Key Events of 2024 – 2035

In the 2024 presidential and parliamentary elections, a completely new political force, unrelated to the past, is likely to win. It would build a future-looking program for Ukraine and a plan to implement it, based on the formation of European values. This includes the process of the dismantling of a traditional political model which in Ukraine comes to an end as the transition to the "direct democracy" tools begins.

The Ukrainian society learns new principles of unity. There would be a new principle of relationship between the Ukrainians: trust and joint action.

Ukraine defeats Russia in the informational struggle both inside the country and the world's informational space. At this time, Russia loses almost all informational levers of influence on both Ukrainian and world societies. The only lever it has – military.

If Ukraine does not join NATO by then and the Russian Federation does not experience an economic downturn, combined with an internal instability in Russian society, there would be a high probability of armed conflict. The Russian Federation would not refuse its geopolitical interests in Ukrainian territory.

However, a Russian Federation victory in the informational space, with the support of the world community and sanctions affecting the Russian economy, is the most likely to avert a direct armed confrontation between Ukraine and Russia.

At the same time, the gap between "fast" and "slow" countries is growing. In some "slow" countries (such as Russia), it leads to internal conflicts. The "slow countries" are trying to slow down the big world, but they no longer have the resources for that.

In 2025-2030, under the burden of internal problems (aggravated by Ukraine's success) and the influence of the world community, the Russian Federation withdraws its protectorate from Donbas and the AR of Crimea, which are returned to Ukraine.

4.3.2.5 Ukraine in 2035

The territorial integrity of Ukraine is restored. Ukraine's informational space is completely controlled by pro-Ukrainian owners. The mass media covers objective information and contributes to the consolidation of the Ukrainian nation.

The world community recognizes Russia as an aggressor, and Ukraine receives reparations from Russia. Global processes of economic transformation have aggravated the systemic socio-economic crisis in the Russian Federation. A series of local conflicts in Russia, aggravated by the economic crisis, led to the loss of the Russian Federation of its geopolitical subjectivity.

Ukraine's assumes more of a regional leadership role and mediator in East-West relations. Ukraine's international authority is partly the result of unique military experience and the ability to successfully reintegrate formerly occupied territories into Ukraine and the body politic.

Humanity comprises the main value in a new Ukrainian state community with personal action for a common goal of Ukrainian sovereignty as the formative principle. Ukrainian society has learned to consolidate to achieve social goals. Public safety is based on people's skills for self-defence and mutual help. There is resocialization of residents from regions that suffered from warfare. Forced migrants from Russia are integrated peacefully into Ukrainian society. Language, national identification, religion, and other issues lost their political meaning and became exclusively a matter of culture and tradition. An effort is made to ensure younger generations have the opportunity to learn English as a second language to prepare them for opportunities more globally.

4.3.3 Scenario No. 2: "Balance on a Rope"

Core Elements:

- Ukraine is not NATO or EU member.
- Ukraine is not a member of the EAC, EAEU, CIS, CSTO.
- The European community's support of Ukraine's Western orientation almost has been lost.
- Ukraine's population supports the informational policy towards Western orientation at a quite high level.
- There has been large-scale aggression of the Union (Common) State (CS) against Ukraine, which poses a threat to international and regional security. The military conflict continues.
- The informational space in Ukraine (except the occupied territories) is protected.

4.3.3.1 Union State (Common State)

The Russian Federation annexes the Republic of Belarus after the long internal conflict, caused by falsified elections in 2020, in effect creating the confederated Common State (CS) originally proposed during Union State precursor discussions.

Formally existing CS makes an active systematic informational pressure on Ukraine and NATO and EU members in order to prevent Ukraine's European and Euro-Atlantic integration. Having chosen a confrontational model, the CS openly uses extremely harsh rhetoric and military force to achieve its goal, as well as the security and intelligence agencies and media. They work towards discrediting Ukraine in the minds of the world community.

Apart from external policy, CS makes appropriate measures within Ukraine to achieve its goals, including Temporarily Occupied Territories (TOT), aimed at changing the current government, returning the political course of Ukraine, and setting the majority of the state towards Russia. Particular attention is paid to the internal political mobilization of the CS population against Ukraine and Ukrainians.

Thus, the CS attempts to achieve its aggressive goal concerning Ukraine, aiming at solving external and internal political issues.

4.3.3.2 Ukraine

The population is consolidated and supports the Western-oriented policy of the state (joining the EU and NATO).

The counteraction to the disinformation of the CS is carried out in close cooperation with supportive countries and their informational sources. They direct and coordinate their collaborative efforts to explain Russia's information actions, as well as to prevent and actively counteract it.

Patriotically oriented people control the mass media and the Internet that improves the objectivity of the informational coverage, assisting in the mitigation of CS propaganda and contributing to the formation of the Ukrainian nation.

4.3.3.3 The Path to 2035

The 2024 presidential and parliamentary elections are likely to be won by political force, which claims the conscious future for Ukraine and has a plan that includes joining the EU and NATO.

Ukrainians support the Western-oriented policy of Ukraine (joining the EU and NATO) and the protection of the informational space. The Ukrainian society would be eager to develop according to the new principles of unity, trust, and common national idea. However, the majority from Donetsk and Luhansk regions would continue to support the CS's informational policy and government.

The CS increasingly lose the levers of informational influence on Ukrainian society. But by approaching NATO borders and deploying short- and medium-range missiles, the possibility of rapid establishing the corridor to Kalininhrad, CS aspires to apply constant pressure, including informational, on Allies and EU. CS policy allows for the exchange of territory and other measures and concessions with the EU as a means of increasing control over Ukraine. The CS government would continue to make efforts in the informational space to persuade the key world players to compromise by resolving the issue of the occupied Ukrainian territories and giving them a right to veto.

Ukraine would gradually lose the support of the European community for Western orientation, as a result of an aggressive CS policy and aggressive CS informational measures. Most of the European countries would recognize the status of Crimea as a part of Russia. In contrast, the USA, Great Britain (non-EU), Canada, Australia, and Israel continue to support the Western policy of Ukraine and do not admit the annexation of Crimea.

The split enhances in the EU, including in the background of CS's informational influence that leads to an increasing level of uncontrolled migration. In this connection, some countries consider the possibility to withdraw from the Union.

Further failure to achieve the goal of destroying Ukrainian statehood by reducing Ukraine's support, may lead to the military aggression of the CS against Ukraine by conducting a strategic offensive (separate special operation).

To justify the open invasion in the Ukrainian territory to the world community, the informational influences are likely to be intensified by carrying out provocations, aimed at discrediting the Armed Forces of Ukraine in the minds of the world community and local population (e.g., propaganda regarding the use of illegal weapons, improper or illegal behavior, extremist elements, etc.). In addition, to destabilize the socio-political situation in other regions, pro-Russian organizations and movements would be intensified in southern and eastern regions, they would provoke protests, disobedience, dissatisfaction with the policy. It can cause a panic and create the image of CS as a "peacekeeping state."

While creating these conditions, the CS would assess the reaction of the world community. If there would be a weakening of Ukraine's international support, condemnation of its actions, the CS's Armed Forces may launch a Special Military Operation under the pretense of "restoring the rights and freedoms of the Russian-speaking population in southern regions of Ukraine and further bringing the "constitutional order" to its territory."

The result of the operation is likely to be the loss of a part of the territory (except isolated districts of the Donetsk and Luhansk regions, the land corridor to the Crimea would be also occupied – part of the Mykolaiv, Kherson, Zaporizhia regions). A resistance movement would be organized at the TOT SOF of the AF of Ukraine that would probably be supported by the local population. The CS would likely continue informational aggression and attempts to influence the political architecture, the results of political choice among Ukrainians both through informational tools (media, social networks) and by supporting the direct and covert henchmen of CS in Ukrainian policy. The main efforts of the CS would seek to implement the "democratic expression of the will of Ukrainians from the eastern-northern regions."

4.3.3.4 Ukraine in 2035

Military conflict continues. The resistance movement is carried out on the TOT. The USA, Great Britain, Canada, Australia, and Israel support Ukraine. The population of Ukraine supports the informational Western policy of Ukraine (mainly joining NATO).

4.3.4 Scenario No. 3: "Little Russia" (Negative)

Core Elements:

- Ukraine refuses to join the EU and NATO;
- The national idea is not formed in Ukrainian society;
- Both Russian and Ukrainian are recognized as state languages;
- There is taking place the delegitimization of the Orthodox Church of Ukraine;
- Ukraine loses the trust of the world community, as a result, they would block their help and support;
- Russia completely controls Ukraine's informational space and influences the formation of values;
- The military conflict ends;
- Ukraine becomes a satellite of the Russian Federation.

4.3.4.1 Ukraine

In this scenario the Ukrainian economy becomes, primarily, a source of raw materials for other countries and fully 100% under Russia's external control. Higher value activities related to science, technology, and industrial activity is controlled for Russia's benefit. Socio-political activity is affected by the heavy influence of Russia, censorship, and total informational control by Russia and Ukrainian proxies, and unchecked corruption undermines society. All media are under the control of curators from the Ministry of Propaganda.

Under such conditions emigration from Ukraine creates negative demographic trends that threaten the long-term viability of the Ukrainian state. The main functions of the government are "policing" and support of the minimal social standard of living for "those who remain." EU countries introduced a visa regime for Ukrainian citizens, while Russia re-establishes visa-free travel between Ukraine and Russia.

4.3.4.2 Russia

An active informational, ideological and physical expansion of Russia and an eventual loss of Ukrainian sovereignty.

4.3.4.3 Key Events of 2020 – 2024

In 2020, the local elections were held in Ukraine, when the populists and revanchists with pro-Russian views gain power. Revanchists take advantage of the deteriorating economy and would advance the idea "bad peace with Russia is better than hopeless war."

The mass media, controlled by pro-Russian owners, try to promote the need for dialogue with leaders in the TOT to shape public opinion about the loss of the military conflict with Russia. At the same time, they create a misbelief among Ukrainians about the historical unity between two fraternal Slavic nations and the negative influence of Western countries on the existence of Russians and Ukrainians. Any political promises made by the Ukrainian government to non-Russian aligned states remain unfulfilled.

Pro-Ukrainian media loses the influence over the Ukrainians. The owners of pro-Ukrainian TV channels and radio stations are under pressure from the government. They are forced to sell their TV channels or leave Ukraine.

At the same time, the powerful influence on the EU informational space enables the development of disagreement and dispute within and between the EU member states. Gradually, more and more EU countries demand withdrawal from the organization. The EU authority puts all efforts into stabilizing the situation inside the EU. In this situation the fate of Ukraine occupies little attention within the EU community. It gradually but rapidly stops its participation in the EU association and other international institutions. Ukrainians emigration to the EU increases and the EU begins considering the reversal of the visa-free regime.

The USA would face the choice between Ukraine and the EU. They would be forced to negotiate with Russia on the issue of ending the destabilization within NATO countries. The USA and EU roll down their support program in Ukraine and release sanctions from Russia in return for ending active information warfare against NATO members.

The Ukrainian government starts negotiations regarding the reintegration of Donbas on the terms of the Russian Federation. Similarly, Ukraine backs down on Crimea at the legislative level. Ukraine returns to Commonwealth of Independent States (CIS).

In 2021 the Ukrainian economy is on the verge of collapse. The last liberals in Ukraine try to gather another Maidan in response to the government activity. Most of the Maidan leaders have been arrested.

In 2022 the government approves a new direction of the Ukrainian economy: agricultural industry and mineral production for export.

Culture, science, and education continue to degrade. Russia's "cultural" product dominates in the informational space.

UOC-MP (Ukrainian Orthodox Church – Moscow Patriarch) gains power and influence to sets the mass propaganda about the unity of Slavic people.

4.3.4.4 Key Events in 2024 – 2035

In 2024, Ukraine holds presidential and parliamentary elections, where pro-Russian politicians and political parties take control of the government. The opposition (patriotic-pro-Ukrainian) bloc is almost absent and has no influence on political life in the country. Corruption is rife throughout all levels of government.

All media are under the control of pro-Russian owners. The Russian sites and social networks, which are under the control of the Russian FSB, are predominant on the Internet. There is active propaganda in Ukraine shaping positive conditions regarding joining the EAEU (Eurasian Economic Union) and CSTO (Collective Security Treaty Organization).

Given the final economic collapse, the government in Ukraine has admitted the Survival Strategy. The Government of Ukraine signs the agreement on joining the EAEU and CSTO.

Academic science is absent. There is no place in Ukraine to get higher education, even in secondary quality. Ukrainian diplomas are not recognized in other countries.

4.3.4.5 Ukraine in 2035

The political system in Ukraine is a form of hidden dictatorship controlled by Russia. Censorship and total information control prevail in Ukraine. All mass media are under the control of pro-Russian owners and serve the government. All mass media are under the control of curators from the Ministry of Propaganda. The decline of journalism and television, combined with attempts to manipulate social networks, has led to greater degradation of Ukrainians' critical thinking and fragmentation of knowledge of factual conditions outside of the country. Ukraine's national cyber capabilities are transformed into an internal punitive detachment.

EU countries introduce a visa regime for Ukraine, and the Russian Federation renewed visa-free travel. Ukraine is a member of CIS, EAEU, and CSTO. The Russian Federation begins the active phase of resettlement in Ukraine, in particular, the large amount of "ethnic Russians."

Corruption transforms the Ukrainian economy into one dominated by bandits and smugglers. Medium business disappeared and small business tries to survive. The bloated budget sphere provides a "state-guaranteed" minimum level of population survival. Ukraine is entirely reliant on economic aid from Russia while large Russian businesses control the major industries in the country. The IT industry is in decline and exists in the form of simple outsourcing for international companies: all intellectual robots are exported to other countries.

Culturally, the history of the "Old Russian state" is studied in schools and any notion of Ukraine as an independent state possessing a unique socio-cultural history is suppressed. Ukrainian identity is denied. The first monument to Putin appears in Ukraine.

Talented people have left the country, the rest serve the production of the raw materials.

The UOC-MP gains power and influence. At that time OCU is recognized as an extremist organization.

4.3.5 Scenario No. 4: "Russian Peace" (Advance of Russian "Peacekeepers")

Core Elements:

- Ukraine's population does not support the state information policy;
- Resistance movements to official authorities emerge and spread in most regions of Ukraine;

- The socio-political situation in Ukraine is partially destabilized;
- The national idea in Ukraine is unformed;
- The Russian Federation has a significant influence in Ukrainian informational space;
- NATO and some other countries continue to support Ukraine's public policy towards European and Euro-Atlantic integration; and
- The Russian Federation advanced its military units in the southeastern regions of Ukraine and positioned them as peacekeepers.

4.3.5.1 Ukraine

Despite the help of the world's leading countries, Ukraine has failed to defeat corruption. The reforms have stalled and have not produced the expected results. There are constant conflicts between different political forces, but "pro-Western" forces win the elections with a slight advantage.

Due to the lack of significant changes in the economy, Ukraine constantly increases its external debt and spends most of the budget on interest payments on external debt services. The standard of living in Ukraine has broken down. Tariffs for energy and utilities are constantly increasing, and prices for food, medicine, and clothing are rising. More than 90% of the population is below the poverty line.

Due to the inconsistency of the promises to improve the lives and the real state of affairs, the constant informational influence of the Russian Federation, and increasing disparities in wages and pensions (not in favor of Ukraine) between Ukraine and the temporarily occupied territories, the Ukrainian population refuses state information policy aimed at Ukraine's accession to the EU and NATO.

The total impoverishment of the Ukrainian population in the background of growing corruption has led to the emergence and spread of resistance movements against the official government. The special operations forces of the Russian Federation support and accompany the resistance movements.

The socio-political situation in Ukraine is partially destabilized (the greatest degree of destabilization is in Donetsk, Luhansk, Zaporizhia, Dnipropetrovsk, Kherson, Mykolaiv, Odesa, Kharkiv, Sumy, Zakarpattia, and Chernivtsi regions).

The program for the development of the Ukrainian language and uniting churches in a single Orthodox Church of Ukraine has been disrupted in most regions of Ukraine. The national idea in Ukrainian society has not progressed. Ukraine's private media structures retransmit the main narratives of Russian propaganda.

The President and the Government of Ukraine are trying to stabilize the situation by continuing to implement the policy (including information policy) aimed at Ukraine's accession to the EU and NATO. Ukraine has imposed a state of emergency and conducts an anti-terrorist operation (in the southeastern regions), which involves some military units (units) of the Armed Forces of Ukraine.

4.3.5.2 Russian Federation

Completion and commissioning of the Nord Stream 2 and South Stream pipelines, as well as the active participation of the Russian Federation in the New Silk Road international project (the Eurasian Land-Bridge), allowed the Russian economy to get out of the crisis caused by international sanctions. The increase in budget revenues allowed the implementation of social programs for the Russian population and, as a result, living standards within the Russian Federation and the illegally occupied territories of Crimea, Donetsk, and Luhansk, have significantly improved.

Russian media structures and information operations forces use the disparity in the standard of living for ordinary citizens in the Russian Federation and Ukraine as one of the main narratives for exerting constant influence on the Ukrainians to demonstrate the benefits of the Eurasian vector. Sub narratives are used: total corruption in Ukrainian society; mobilization of the force structures by the Ukrainian military-political government against its people (during the anti-terrorist operation); the inability of the Ukrainian "pro-Western" government to stabilize the situation in the country.

Corruption among the highest echelons of Ukrainian authority has allowed Russian media outlets to buy out controlling stocks from leading Ukrainian media and, as a result, dominate Ukraine's information space.

Taking advantage of the inability to stabilize the situation in the country by Ukrainian authorities, drawing on calls by pro-Russian movements for the intervention of international peacekeeping forces to Ukraine (to prevent mass repression of civilians, humanitarian crises, and disasters), the Russian Federation advances military forces into Ukraine.

4.3.5.3 World Community

NATO and some other countries: the USA, Canada, Great Britain, Australia, Poland continue to support Ukraine's state policy aimed at European and Euro-Atlantic integration to prevent Ukraine from returning to Russian control and deterring Russian expansion into Europe.

Hungary and Romania, using the destabilization in the socio-political situation in Zakarpattia, Chernivtsi, and Odesa regions, increase their informational influence on international security organizations, urging them to promote cultural autonomy for ethnic Romanians (Chernivtsi, partly Odessa regions) and Hungarians (Zakarpattia region) on the Ukrainian territory under the protectorate of Romania and Hungary, respectively. All NATO decisions on Ukraine are blocked by these countries.

France, Germany, and other EU countries have focused on preserving the integrity of the EU. These countries question NATO's ability to ensure the military defence of Europe. This position is partly based on the Russian Federation's successful information campaigns against EU leaders and populations. Under the influence of Russian narratives about the benefits of economic cooperation in the Eurasian Union format, threats to regional security in Europe, they have taken a wait-and-see neutral position on the Russian-Ukrainian conflict.

China is interested in the development of economic relations within the international project "New Silk Road" and therefore supports the Russian Federation in the development of Eurasian cooperation.

4.4 SUMMARY

Thus, the current situation (circa 2019/2020) contains preconditions for several variants of the possible political situation around Ukraine under armed aggression by the Russian Federation. However, in the coming years, this future would be limited by two unlikely key constants – large-scale armed aggression by the Union (Common) State and the final settlement of the political situation between Ukraine and Russia.

During the research, the authors identified the two most influential groups of factors, which determine the informational aspect of the military conflict between the Russian Federation and Ukraine: the attitude of leading countries and international security organizations to Ukraine and the perception of the state policy by Ukrainians.

Based on the study, it is possible to determine that, firstly, Ukraine would be constantly under Russia's informational influence, secondly, Ukraine's informational space is insufficiently protected from the influence of the Russian Federation, thirdly, the Ukrainian national idea remains insufficiently supported

across Ukrainian society. These conditions create the necessity to implement a set of actions to ensure the informational security of Ukraine. The realization of this plan would create the conditions for the sustainable and guaranteed satisfaction of national interests, would allow the identification, prevention, and neutralization of threats to Ukraine's national interests and national security in the informational sphere.

The selected complex factors make it possible to obtain one baseline and four derivative scenarios of the situation, namely:

1) **"Slow movement" –** to preserve insufficiently stable democratic development in Ukraine and bring into question its affiliation to the European political tradition while preserving the current level of support by the EU and the USA.
2) **"Independence" (positive) –** a steady increase in the stable democratic development (Ukraine's accession to the EU and NATO) while increasing the level of trust and support by the world community and protecting Ukraine's informational space.
3) **"Balancing on the rope" –** destabilizing the democratic development in the country in the background of large-scale aggression of the Union (Common) State against Ukraine and practical loss of support by the European community.
4) **"Little Russia" (negative) –** the destruction of Ukraine's democratic development (Ukraine becomes a satellite of the Russian Federation), Ukraine loses its confidence in the world community's sight, which is why they block their assistance and support.
5) **"Russian peace" (advance of Russian "peacekeepers") –** despite the continued support of Ukraine's pro-European state policy by NATO and other countries, there is the destabilization in the socio-political situation while the advancing of the so-called "peacekeeping forces" by Russia.

The assessment of possible scenarios shows that there would be some combined variant in reality with the separate features of the proposed scenarios. The probability of future events by each scenario is approximately the same and depends on the 2020 local elections in Ukraine, 2024 presidential and parliamentary elections, possibly early elections to the Verkhovna Rada, etc. However, the probability of the large-scale armed conflict between Russia and Ukraine is very high under the scenario "Balancing on the rope."

A scenario that combines two influential, unpredictable factors with different effects is defined as unstable.

The best course of events in Ukraine is based on the "Independence" scenario.

4.5 BIBLIOGRAPHY

[1] Zgurovsky, M., Boldak, A., Melnyk, O. et al. "Foresight 2018: Systemic World Conflicts and Global Forecast for XXI Century." International Council for Science: NTUU "Igor Sikorsky Kyiv Polytechnic Institute," 2018.

[2] The Russian Federation Military Doctrine, Approved by the President of the RF from 25.12.2014 N П, p. 2976.

[3] Ukraine Military Doctrine, Approved by the Decree of the President of Ukraine from September 24, 2015, No. 555/2015.

[4] Gorbulin, V. "Abstracts to the Second Anniversary of the Russian Aggression Against Ukraine." [digital resource]. https://docviewer.yandex.ua/view

[5] The Doctrine of Informational Security of the Russian Federation, Approved by the Decree of the President of the Russian Federation from 5.12.2016 No. 646.

[6] The Doctrine of Informational Security of Ukraine, approved by the Decree of the President of Ukraine from February 25, 2017, No. 47/2017.

[7] Podberezkin, A.I. et al. "Long-Term Forecasting of the International Situation: Analytical Report." Moscow, State Institute of the International Relations (University) of the Ministry of Foreign Affairs of Russia, Center for Military and Political Studies. MGIMO – Universitet, 2014.

[8] Drach, I. "How to Arrange the Informational Space." Man and Power, 1-2, 2001, p.68.

[9] Zolotukhin, D.Y. "The White Book of Special Information Operations Against Ukraine 2014 – 2018." Ministry of Information Policy, 2018.

[10] Kremlin Informational Influence Index, Media Detector GO Report. https://ms.detector.media/mediaprosvita/research/indeks_informatsiynogo_vplivu_kremlya/ Accessed 30 November 2023

[11] The Concept of the Russian Federation Foreign Policy, Approved by the Decree of the President of the Russian Federation dated 30 November 2016, No. 640.

[12] "We Need Many and Different Newspapers. But Our Own." Ukrainian Independent View, 27 June 1998.

[13] About the National Purposes and Strategic Tasks of the Russian Federation Development until 2024, Approved by the Decree of the President of the Russian Federation from 05/07/2018 No. 204;

[14] A forecast of socio-economic development of the Russian Federation for the period up to 2036, Ministry of Economic Development of the Russian Federation, 2016.

[15] Podberezkin, A.I., Alexandrova, M.V. (eds.) Strategic Forecasting of International Relations. Monograph. Moscow, State Institute of International Relations. Ministry of Foreign Affairs of the Russian Federation, Center for Military and Political Studies. MGIMO Universitet, 2016.

[16] National Security Strategy in the Russian Federation, Approved by the Decree of the President of the Russian Federation from 28 June 2014, No. 683.

[17] Spatial Development Strategy in the Russian Federation for the Period until 2025, Approved by the Government Executive Order of the Russian Federation from February 13, 2019, No. 207.

[18] Strategic Defense Bulletin of Ukraine, Enacted by the Decree of the President of Ukraine from June 6, 2016, No. 240\2016.

[19] Cybersecurity Strategy in Ukraine, Approved by the Decree of the President of Ukraine from March 15, 2016, No. 96\2016.

[20] National Security Strategy in Ukraine, Approved by the Decree of the President of Ukraine from May 26, 2015, No. 287\2015.

[21] Development Strategy of the Defense-Industrial Complex in Ukraine for the Period until 2028, Approved by the order of the Cabinet of Ministers of Ukraine from June 20, 2018, No. 442.

[22] Zhurovskyi, M.Z. "Foresight and Building a Strategy of Socio-Economic Development of Ukraine on Medium-Term (to 2020) and Long-Term (to 2030) Time Horizons." International Council on Science, Committee on System Analysis under the Presidium of the NAS of Ukraine, National Technical University of Ukraine "Kyiv Polytechnic Institute Ihor Sikorskyi," Institute of Applied System Analysis, MES and NAS of Ukraine, World Data Center for Geoinformatics and Sustainable Development; Agrarian Superstate Foundation. Politekhnika, 2016.

[23] Central Research Institute of the Armed Forces of Ukraine (CRSI of AFU). "Informational and Analytical Materials for the Preliminary Description of the Future Security Environment 'Future Security Environment 2030. Analysis of Strategic Prediction'." 2019.

[24] Martyniuk, V. (Ed.) "Hybrid Threats to Ukraine and Public Security. EU and Eastern Partnership Experience." Analytical document. Kyiv, 2018. https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/blok_XXI-end_0202.pdf

Chapter 5 – CREEPING NORMALITY: RUSSIA'S USE OF INFORMATION CONFRONTATION AGAINST THE CANADIAN ARMED FORCES IN LATVIA AND UKRAINE

Matthew A. Lauder
Defence Research and Development Canada – Toronto Research Centre
CANADA

5.1 INTRODUCTION

While several military analysts have made rather ominous predictions and warned of a Russian military invasion and occupation of the Baltic states, a close examination of Russia's military activities across Eastern and Central Europe, as well as Caucasia, over the last two decades suggests that such a scenario – while plausible – is unlikely [1], [2], [3]. In short, a full-scale invasion or even limited, conventional military intervention and the direct use of armed violence (which some analysts argue is employed by the Russian government only as a last resort) against the Baltic states would not achieve Russia's long-term geopolitical objectives [4]. Moreover, not only would an invasion trigger NATO collective defence efforts but Russia's recent experience in Ukraine clearly demonstrates it does not have the force structure, personnel, and lines of communication to occupy and control large geographic areas with dense population bases) [5]. This does not mean that Russia is not a direct or explicit threat to the security and sovereignty of the Baltic states – quite the opposite, in fact. Rather than using conventional military capabilities and armed violence, however, the Russian government is actively engaged in an enduring, pervasive, and largely covert campaign to subvert the Baltic states by undermining social, political, military, and economic structures, including the relationship between the host country and its population and that of NATO [6], [7], [8]. Often referred to as *sub-threshold conflict*, as well as *hybrid warfare*, *grey zone operations*, *political warfare*, *new generation warfare*, *non-linear warfare* and the *Gerasimov doctrine*, this multifaceted and obfuscated campaign is grounded in information warfare – or what is generally referred to as *information confrontation* in Russian military parlance – which includes but is not limited to the employment of propaganda, disinformation and influence operations (including physical demonstrations designed to intimidate, such as military build-ups, exercises and flyovers) as well as offensive cyber activities and other technological interventions across the electro-magnetic spectrum, such as jamming/disruption, reconnaissance, and intelligence collection [9], [10], [11].

In support of *NATO SAS-RTG-161 – Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices*, the purpose of this chapter is to briefly examine the operational context, mechanics and impact of Russian information confrontation targeting the Canadian Armed Forces in Central and Eastern Europe, specifically the missions in Latvia and Ukraine (Operation REASURRANCE and Operation UNIFIER, respectively).[1] To achieve this objective, this report is

[1] As a single case study within a much larger compendium of research, this paper is only meant to provide a concise examination of Russian information confrontation employed against the Canadian Armed Forces in Eastern and Central Europe. To achieve this goal, this paper discusses specific but limited aspects of the problem, namely Russian strategic doctrine that speaks to or informs the employment of information confrontation as well as some socio-technical models depicting how these high-level concepts and are operationalized to generate desired effects. Unfortunately, due to space limitations, a discussion – even a limited one - of Russian military capability proponents and the impact of military theory (i.e., Russian military science) on the design and execution of information confrontation is not possible. As such, this paper should not be considered a definitive account or discussion of the topic, but rather a glimpse into the problem and utilized as a springboard for more detailed and comprehensive examinations. It should also be noted that this study draws upon work previously published by Defence Research and Development Canada, much of which is restricted and not available for public distribution.

divided into two broad but complementary sections. The first section briefly outlines the strategic doctrine, organizational structure, and forms or manifestations of information confrontation and presents a sociotechnical model of target audience manipulation employed by the Russian government to generate disruptive effects, such as creating and amplifying social and political discontent and mobilizing people towards violence. Due to space limitation, a more detailed discussion of the operational and strategic context of information confrontation is beyond the remit of this chapter. The second section examines seven exemplary incidents in which the Russian government, and/or its proxies, employed information confrontation for the purposes of attacking and undermining the credibility of the Canadian Armed Forces and, by extension, NATO in Latvia and Ukraine. To demonstrate the robust nature of Russian information confrontation, this section also identifies a number of other incidents targeting NATO missions, military personnel, political leaders and government institutions in the Baltic states and Ukraine. This report concludes with a short summary that identifies and discusses two key implications of and practical recommendations to respond to Russian information confrontation.[2]

5.2 RUSSIAN INFORMATION CONFRONTATION

Recognizing critical deficiencies in its ability to generate effects through the information space during several conflicts, notably the First and Second Chechen Wars (1994 – 1996 and 1999 – 2009, respectively) and the Russo-Georgian War (2008) and concerned about US and NATO applications of (e.g., in support of color revolutions) and advancements in information warfare, the Russian government has made significant investments in information confrontation, in particular over the last decade [6], [9].[3] This revitalization effort included the implementation of new organizational structures and doctrine, but also the development and employment of new capabilities and tactics, including refreshing underpinning concepts and theories, as well as developing a new approach to decentralized command and control (C2) of informational capabilities, or what can also be referred to as distributed control [16]. The Russian government also started to outsource information confrontation, effectively handing over (at least some) responsibility to design and execute activities to a range of non-state actors, including news media agencies, organized crime networks, Private Military Corporations (PMCs), and patriotic and religious organizations, just to name a few [9], [17], [18]. The outcome of revitalization effort is a decentralized, seemingly pervasive and highly agile approach to information confrontation that fully embraces both a Whole-of-Society (WoS) approach as well as political risk, in particular potential negative media coverage from failed or uncovered activities (e.g., exposure of GRU involvement in attempted Skripal assassination, involvement in Czech Republic bombings in 2014, or the attempted coup in Montenegro in 2016) [19], [20], [21]. It should be noted that the contemporary approach is in stark contrast to how information warfare (sometime referred to as psychological warfare) was conducted during the Soviet era, which was strictly hierarchical; that is, with clear lanes of responsibility between security, military and political organizations and direction coming from the highest level of government (e.g., the Politburo and the Secretariate of the Communist Party of the Soviet Union [CPSU]) [6]. However, while there are clear structural and operational differences, many – albeit not all – of the underpinning concepts and theories of contemporary Russian information confrontation can be found

[2] This report draws upon and is informed by more than eight years of dedicated adversarial intent research on state and non-state asymmetric capabilities conducted under the auspices of the Socio-Cultural Intelligence support to Joint Tactical Targeting (SOCINT) and Adversarial Asymmetric Advantage and Rapid Countermeasures (A3RCOM) projects conducted by the Toronto Research Centre, Defence Research and Development Canada (DRDC). It should be noted that many of the publications generated by DRDC are not intended for broad distribution and therefore are not accessible to the public.

[3] Several authors offer detailed examinations of how the Russian government perceives the US and NATO as a threat to its national sovereignty as well as its military build-up and revival, including Jonnson (2019) [12], Adamsky (2010) [13], Retz (2018) [14], and Bērziņš (2019) [15].

in Soviet information warfare, most notably reflexive control[4] and subversion theory[5], [8], [9], [22], [23].[6] Coupled with a highly agile operating approach that allows the Russian government to adapt and quickly evolve capabilities and tactics and identify and exploit opportunities and adversary vulnerabilities, the end result is – for all intents and purposes – a new approach to information warfare, one explicitly designed for and exploiting the *post-truth era* [24].[7]

5.2.1 Doctrine and Policy

The Russian government has not published information confrontation doctrine; that is, the Russian military equivalent of NATO's Allied Joint Doctrine on Information Operations, or *AJP-3.10*. That, however, does not mean information confrontation doctrine does not exist; rather, it is not publicly accessible (Russian operational and tactical doctrine tends to be classified). Although called *doctrine* by the Russian government, what is published and publicly accessible is less doctrine (at least from a Western military perspective) and more strategic policy and guidance. That being said, the Russian government has clearly articulated, evolved and broadened the scope of its strategic level defence and security guidance in the form of a series of policy statements, with specific references to information confrontation and activities conducted in the information space. In most instances, the strategic documents are also not specific to the military but rather identify and discuss the role of state, quasi-state and non-state entities of the federal government in the physical and psychological defence of Russia, and its allies. To help frame the discussion of incidents identified in section two, this section provides a brief examination of the most significant concepts discussed in strategic policy regarding information confrontation, which includes both technological and psychological interventions. It is important to note that, due to conceptual and theoretical overlap as well as their transformative nature, the documents should not be read in isolation but rather as an evolving body-of-work. In other words, it is by examining the totality of documents that the breadth and the nuances of information confrontation, and its role in maintaining Russian national sovereignty and territorial integrity, can be appreciated. Due to space limitations, this section does not provide a comprehensive analysis of the strategic documents; rather, it identifies and briefly discusses the parts most relevant to the design, operationalization and execution of information confrontation.

5.2.1.1 National Security Concept (2000)

Approved in January 2000 and integrating lessons from the conflicts in the Balkans and Chechnya, the document identifies a number of internal and external threats to the Russian Federation and its allies, including social and political polarization, organized crime, terrorism and interethnic conflict, as well as NATO expansion, the proliferation of weapons of mass destruction and the weakening of Russia's international political, economic and military influence. The document also recognizes the emergence of several threats to national security in the "information sphere" [25]. The concept further identifies attempts by a number of unnamed countries to "dominate the global information space and oust Russia from the information market" and also the development of "information wars," which includes attacks upon and

[4] Reflexive control is a computational technique developed in the early 1960s by the KGB for the design and planning of activities to manipulate a target through information and perception management. Reflexive control is based on the following three principles: 1) That the instigators of the activity have a detailed understanding of the target, including psychological vulnerabilities; 2) That the target has no knowledge or awareness of the manipulation; and 3) That the system of interaction between instigator and target is dynamic, which requires inherent flexibility and agility in information delivery.

[5] Subversion theory was developed during the Soviet era and is an ideological warfare tool designed to defeat the competing political-economic system of capitalism. Subversion theory is based on the idea that all elements of national power can be used to undermine the integrity of system structures of an adversary/target nation and achieve geopolitical goals, but in such a way that the subversive activities remain under the threshold of formal or declared war.

[6] It should be noted that Russian information confrontation is not entirely new but grounded in scientific research conducted by the Soviet Union. For an examination of the historical and scientific antecedents of Russian information confrontation, see [22], [23].

[7] Post-truth era is a philosophical and political concept indicating the replacement of shared or common standards of objective truth with opinion, emotion, personal belief or alternative facts or fake news.

disruption of information and telecommunications systems. Moreover, the concept mentions the threat of the development of a new generation of weapons, coupled with "radical changes in the forms and methods of warfare" [25].

In response to these threats, the concept identifies the Russian government will actively seek to prevent wars and armed conflict through several actions, including the pre-emptive application of political, diplomatic, economic and other non-military means, as well as protecting or defending information infrastructure, continuing to integrate Russian capabilities into the global information space, and actively countering rivals in the information space [25]. It is important to note that this is the first mention in strategic doctrine and policy, since the collapse of the Soviet Union, of threats to the information space, as well as the requirement to take pre-emptive action, using a broad range of non-military means, in the defence of the Russian Federation.

5.2.1.2 Russian Military Doctrine

The 2000 Russian military doctrine largely focuses on updating and expanding the provisions on the use of nuclear weapons as a means of deterrence against aggression by state actors and to ensure international stability. While defensive in nature, the doctrine effectively lowers the threshold for the employment of nuclear weapons, stating the Russian Federation reserves the right to use nuclear weapons in response to state aggression, particularly – but not limited to – the use of weapons of mass destruction and to pre-empt and prevent war. In other words, the military doctrine makes it clear the Russian government retains the right of first strike under certain (albeit broad) circumstances, including the defence of allies and other conventional attacks that threaten national security, geographic integrity and political sovereignty. The doctrine also identifies four main types of warfare; that of

1) *Armed conflict* conducted by ethnic or religious groups for the purposes of destabilizing a country,
2) *Local war*, characterized by one or more states attempting to achieve limited political outcomes,
3) *Regional war*, which involves a state or coalition pursuing geopolitical objectives, and
4) *Global war*, characterized by an existential struggle for survival [26].

The doctrine notes that the use of nuclear weapons is justified in both regional and global wars.

The doctrine also identifies a number of threats to the Russian Federation, including the expansion of military blocs and alliances, introduction of foreign troops in violation of the United Nations (UN) Charter, international terrorism, extremist groups, and organized crime. However, the doctrine also identifies hostile information operations as a primary threat to Russia.

5.2.1.3 Foreign Policy Concept (2000)

Approved in June 2000, the Foreign Policy Concept can be divided into two thematic sections. The first section identifies a number of threats to Russian national security, including military-political rivalry between regional powers, the emergence and growth of separatist, ethnic-national and religious extremist movements, and the use of economic, political, scientific, ecological and informational factors as an adjunct to military power, with the objective of undermining global security. The second section of the concept discusses a number of global and regional priorities, including working with NATO to ensure security and stability across Europe [27]. This portion of the concept also notes the requirement for information support to Russian foreign policy activities. This includes, but is not limited to, communicating what the Russian government determines as accurate information and "forming a positive perception of Russia abroad" [27]. Importantly, the concept identifies the requirement for the Russian government to develop its own means of "informational influence" to shape international public opinion [27].

5.2.1.4 Information Security Doctrine (2000)

Approved in September 2000, the doctrine outlines the goals and principles for ensuring information security. Defensive in nature, the purpose of the doctrine is to ensure the spiritual renewal of Russia, preserve territorial integrity and maintain social and economic stability [28]. The doctrine identifies several key concerns, including retaining the *moral fabric* of Russian society and the historical tradition of patriotism. The doctrine also argues the state is required to prohibit or limit the ability of actors to disseminate propaganda or engage in campaigns to foment social unrest in Russia [28]. Similar to the foreign policy concept, the doctrine also posits the requirement of the state to expand national mass media capabilities to convey "reliable information" to both Russian and foreign citizens (i.e., international audiences) [28].

Similar to other strategic documents, the doctrine identifies a number of threats to the Russian Federation, in particular threats to Russia's patriotic and spiritual renewal as well as the promotion of moral values contrary to traditional Russian society" [28]. The Russian government also recognizes attempts by unnamed external actors to block Russian state media and the development and proliferation of information weapons, ostensibly to undermine the patriotic, spiritual and moral character of Russian society.

5.2.1.5 Conceptual Views on the Activity of the Russian Federation Armed Forces in the Information Space (2011)

Advancing concepts initially promoted in the information security document released in 2000, which served as the first official blueprint for the Russian government to understand and operate in the informational space, the Russian military published its own doctrine in 2011. Although not information confrontation doctrine per se, the document does discuss a number of core concepts of information warfare. For example, the concept identifies "military conflict" in the information space as a "form of interstate or intrastate conflict" through the application and employment of "information weapons," which includes but is not limited to cyber activities [29]. The doctrine also describes information warfare as a "confrontation between two or more states in the information space" with the objective of damaging information systems (networks and repositories), undermining political, economic and social structures, as well as the "psychological manipulation of the population to destabilize the state" and to coerce the state to make decisions or policies to the benefit of its adversaries [29]. The doctrine further defines information weapons as "technologies, means and methods" employed in the execution of information warfare [29].

5.2.1.6 Military Doctrine of the Russian Federation (2014)

The 2014 edition of the military doctrine integrates and revises several concepts from previous strategic documents and also updates and discusses a wide range of threats and risks to the Russian Federation.[8] For example, the doctrine notes that while large-scale war is less likely, military risks and threats have shifted to the information space and the domestic environment of the Russian Federation [30]. In a departure from previous documents, the doctrine explicitly identifies NATO enlargement and encroachment, as well as attempts by unnamed foreign entities to overthrow and destabilize legitimate and allied governments and states (via color revolutions enabled by information and communication technologies), as a significant and evolving threat to Russian sovereignty. Although the foreign entities and allied governments were not identified in the doctrine, many analysts interpret the statement was a reference to Euromaidan and perceived Western interference [9], [12], [31], [32].

The doctrine also advances the Russian understanding of the evolving character of contemporary military conflict, which is characterized by the integrated use of military and non-military means (e.g., political, economic, informational, etc.), as well as foreign-funded political groups and non-governmental

[8] Jonnson [12] examines Russia's signalling to the West through the strategic documents, including its intent to develop military capabilities in response to perceived threats, and Lauder [9] offers an account of how the Russian government frames capability development and engages in theoretical and conceptual discourse.

organizations, irregular forces and private military corporations to amplify and support the "protest potential of the population" [30]. The doctrine also notes that traditional military means have been replaced by indirect and other approaches, including activities in the information space. Interestingly, the doctrine points out that it is the main task of the Russian military to neutralize these threats – at least initially – through the application of political, diplomatic, and other non-military means, specifically the use of information and communications technologies.

5.2.1.7 Russian Federation's National Security Strategy (2015)

Approved in December 2015, the strategy document builds upon the 2011 version and recognizes increased tension and the potential for conflict between the West and the Russian Federation [33]. For example, the strategy asserts that the West is purposefully creating political upheaval and tension in Eurasia, which is negatively impacting Russia [33]. Moreover, the strategy explicitly blames the continuing conflict in Ukraine on the West, specifically the US and European Union (EU). The strategy also warns that overthrowing of political regimes by fomenting revolutions is increasingly widespread [33].

Similar to the military doctrine (2014), the strategy identifies a number of threats to the Russian Federation, as well as the main tasks of the Russian government in response to these threats. In addition to the threat posed by extremist organizations, the strategy identifies "radical public associations" and foreign funded or sponsored non-government organizations as a threat to the Russian Federation, namely because they are recognized as undermining social, religious and moral unity and the primary catalyst of color revolutions [33]. In addition, the strategy acknowledges information and communication technologies as a threat to the Russian government, in particular when they are used to disseminate and promote ideas that undermine the political and social stability in Russia [33].

5.2.1.8 Foreign Policy Concept of the Russian Federation (2016)

The strategic document largely reflects the issues and threats identified in other documents, noting that numerous but unspecified countries are using a range of military and non-military means, including economic, cultural, legal, technological and informational, to achieve foreign policy objectives [34]. The document also identifies and discusses a number of objectives for the Russian government, including strengthening Russia's geopolitical influence, promoting the Russian language and cultural identity of the Russian people, and defending the rights of the Russian-speaking diaspora (e.g., emphasizing and promoting the concepts of Russkiy Mir and Russian compatriots).[9] Like previous documents, the 2016 version argues the Russian government will enhance and promote the standing of Russian mass media and communications tools in order to promote Russia's perspective [34]. Moreover, the document expresses concern about a lack of objective coverage of and discourse about Russia, Russian foreign policy and Russian actions abroad, and that the Russian government must develop its own means to influence international audiences, ostensibly to counter propaganda and disinformation disseminated by state competitors (i.e., the West) [34].

5.2.1.9 Doctrine of Information Security of the Russian Federation (2016)

Building upon the information doctrine released in 2000 and the information space concept of 2011, the 2016 information security doctrine is largely an update of key concepts and definitions. For example, the doctrine comprehensively defines the information sphere as information, information objects, information

[9] Russkiy Mir, literally Russian World, is a core concept of the Russian government, the objective of which is to promote and maintain Russian history, culture, religion, language, and other social and political traditions on the international stage, and to advocate for the rights of Russian ethnolinguistic populations outside of Russia. Russkiy Mir Foundation is also a Government-Organized Non-Governmental Organization (GONGO) that is used to promote Russian culture abroad but has been known to conduct or support information confrontation and intelligence activities on behalf of the Russian government. The concept of Russian compatriots, specifically the protection of Russian ethnolinguistic populations living abroad, is a key component of Russkiy Mir, as well as foreign and security policy, more generally, and is often invoked by the Russian government as a justification for potential military intervention.

systems, websites, communications networks, information technologies, as well as the entities involved in the generation and processing of information, efforts to develop information technology and the mechanisms to regulate access, control and dissemination of information. Likewise, the doctrine defines information threats as the actions and factors designed to damage national interests in the information sphere, including biased and negative information about Russia and the Russian government [35].

In response to these threats, the doctrine explicitly identifies the role of the Russian government as facilitating the development of an information security systems to counter foreign information and psychological actions, specifically attempts to undermine the Russian cultural and patriotic identity [35]. These defensive activities include, but are not limited to, neutralizing attempts by entities (state and non-state actors) to undermine Russian "traditional moral and spiritual values" and providing Russians and the international community with reliable and objective information about the Russian state [35]. Lastly, the doctrine identifies the requirement of the Russian government to control and reinforce traditional spiritual and moral values, including the provision of youth-focused patriotic education programs.

5.2.1.10 Observations

Before proceeding with a discussion of the structure and the underpinning conceptual model of information confrontation, it is important to note the following observations:

1) Russian doctrine typically frames the offensive application of offensive military force as a defensive measure, including pre-emptive actions to deter, prevent or suppress aggression against Russia and its allies. This approach is not novel and follows Soviet tradition of seeking advantage through surprise, but is applied across the breadth of military means and capabilities, in particular information confrontation;

2) The Russian government has developed a holistic understanding of the operating environment and promotes a concept of common defence that includes military, economic, political, informational and other (i.e., non-military) means;

3) Although there appears to be a lack of consistency across strategic doctrine and policies regarding how terms and concepts are applied, the Russian government generally differentiates between "information" and "psychological" aspects of information confrontation (sometimes called information-technical and information-psychological, respectively). In short, information refers to the technical means of collecting, processing, storing, analyzing and disseminating information, including changes to or alterations in data and information, whereas psychological aspects refer to techniques or actions that bring about a change in how a target or target audience thinks and behaves. It is also important to note that these are highly interdependent concepts and rarely discussed in isolation;

4) Russian doctrine does not use the term cyberwarfare, rather it discusses technological interventions in the information space. The implication is that the Russian government conceives of cyber warfare as inherently different from other types or forms of information warfare, as is the case in the West;

5) Military and political objectives are inherently connected, and the military plays a significant role in achieving geopolitical objectives; and,

6) At the core of so-called defensive activities in response to perceived foreign informational threats is the requirement to preserve the domestic information environment, specifically the cultural, spiritual, moral and patriotic unity of the Russian Federation.

5.2.2 Information Confrontation: Structure and Employment

From a functional perspective, Russian information confrontation can be divided into three complementary forms of activity; that of: a) Maskirovka; b) Active measures and C0 Strategic information, also known as strategic disinformation or propaganda (see Figure 5-1) [6], [7].

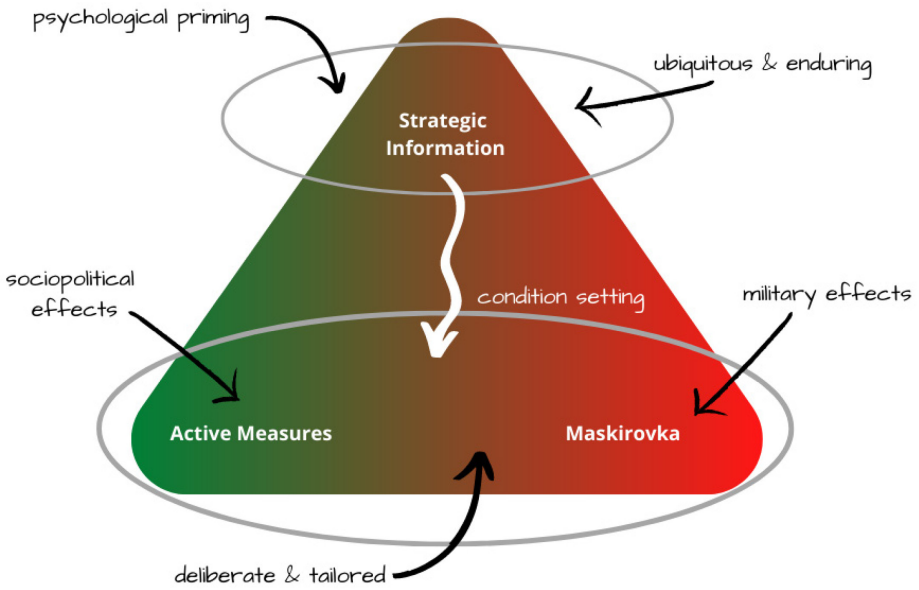

Figure 5-1: Forms of Activity of Russian Information Confrontation.

Maskirovka (more commonly referred to as military deception) has a long history in Russia and the Soviet Union and is applied to generate tailored military effects, such as disrupting enemy force command and control (C2) or undermining electronic surveillance and reconnaissance capabilities. Maskirovka was also used to undermine the will and morale of enemy forces, or what is referred to as combat psychological operations (combat PSYOPS) in NATO. In some cases, maskirovka can be used against the civilian population, but this is generally done to (indirectly) shape how the enemy force perceives a given situation. Traditionally, maskirovka was remit of the GRU (*Glavnoye razvedyvatel'noye upravleniye* or the Main Intelligence Directorate) and was divided into four tactics and applied at all levels of operations, that of:

1) Camouflage and concealment;
2) Demonstrations and feints;
3) Imitation (e.g., false radio traffic); and
4) Disinformation (e.g., psychological activities meant to undermine enemy morale or targeted campaigns to undermine the credibility of the leadership of the enemy force).

However, several differences exist between traditional and contemporary conceptualizations of maskirovka. For example, examinations of recent military and GRU related operations, such as Estonia (Bronze Soldier riots in 2007), Georgia (invasion in 2008), Ukraine (invasion and occupation from 2014 to present), Syria (military operations from 2015 to present), United Kingdom (attempted assassination of Sergei Skripal, 2018), Montenegro (attempted coup, 2018), and the Netherlands (attempted cyber-attack on the Organization for the Prohibition of Chemical Weapons [OPCW], 2018) indicates the GRU conducts an expanded range of activities, and has broadened its target set, in foreign nations, including purely civilian targets (i.e., a target with little or questionable military value) and generating strategic political effects. Moreover, the number and type of entities involved in the design and execution of maskirovka has increased to include the FSB

(Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii, or the Federal Security Service) as well as a range of non-state actors (e.g., Night Wolves, Wagner Group, NASHI, Internet Research Agency, and the Russian Business Network) (this is largely due to the contracting out of traditional military and intelligence activities) [17]. In addition to conducting information confrontation and facilitating military deception activities, non-state actors, in particular private military corporations and patriotic groups – sometimes operating under the guise of self-defence groups – are being employed by the Russian military to support or conduct tactical military activities (e.g., armed raids) as part of a combined forces campaign. In some cases, trusted non-state actors, which are usually made up of former military or security service personnel, have conducted operations independent of the Russian military, such as the Night Wolves and the Rubezh in Crimea and Wagner in eastern Ukraine, Syria and Africa [17], [18], [36].

Whereas maskirovka was the remit of the GRU, active measures were the sole responsibility of the KGB (*Komitet Gosudarstvennoy Bezopasnosti*, or the Committee for State Security) and conducted to generate broader (i.e., strategic) social and political effects, typically by targeting a nation's civilian population or political, cultural and business elite. Traditionally, active measures were divided into three tactics or approaches; that of a) Propaganda (exploited mass media and used forged or falsified documents to shape public opinion); b) Disinformation (exploited stereotypes but otherwise grounded in reality); and c) Influence operations (targeted campaigns to leverage elites, either wittingly or unwittingly, to influence decision-making and policy development). Although conceptually distinct, in practice the three forms were often blended or executed in a complementary fashion to generate desired effects, such as changing public opinion.

An examination of contemporary active measures campaigns in Europe and North America, however, clearly indicates several fundamental changes. Firstly, the design and execution of active measures are no longer the domain of state security services but are now conducted by a range of state and non-state actors, including the GRU and the Ministry of Foreign Affairs (MFA), as well as pro-Kremlin media outlets and other business enterprises (including financial institutions), non-profit and patriotic organizations, as well as hacker groups and criminal organizations [8], [18]. Second, active measures are also no longer limited to employment at or directed towards the strategic level; rather, they are now utilized to generate disruptive social and political effects at all levels of operations (e.g., attempts to undermine or eliminate local politicians and social justice advocates, disrupting or undermining businesses, and encouraging localized riots and looting to undermine the credibility of civilian police and security agencies). Lastly, the tactics employed in active measures campaigns have also increased significantly to include direct action, provocation, ideological subversion, character assassination (also known as smear campaigns, *black PR* and *kompromat*), blackmail, information sabotage and network (social and virtual) destruction, amongst others [37].[10]

In contrast, strategic information activities (also referred to as strategic propaganda) are ubiquitous and enduring form of high-level information confrontation. However, strategic information activities play a critical role in that they set conditions for active measures and maskirovka. In other words, strategic information activities are not designed to generate an effect on their own, but rather to psychologically prime target audiences through narratives. Strategic information activities, therefore, serves to condition target audiences to be receptive to maskirovka and action measures [7].

Similar to the other forms of information confrontation, both state and non-state entities are utilized for the design and operationalization of strategic information activities. These entities include, but are not limited to, government departments (e.g., MFA), government-control and private news media agencies (e.g., *RT*, *Sputnik*, *TASS*, *Isvestia*, Internet Research Agency [also known as IRA, Glavset and the *Federal News Agency*], and *Vesti News*), non-profit and government organized non-governmental agencies (e.g., Russkiy Mir), patriotic groups (Nightwolves) as well as a number of academic and scholarly institutions and foreign-operated agencies

[10] There are a number of reasons for the development of new tactics, such as technological advancements (e.g., the internet, social media applications, peer-2-peer networks, advanced datamining analytics, etc.), the democratization of the media (i.e., the introduction of citizen and advocacy journalism) and changing societal notions of trust in information sources and the questioning of truth (e.g., the post-truth era).

(e.g., Katehon, RAPI and Global Research) [18]. Moreover, some media organizations, such as the IRA, also curate a range of fake online personas (often disguised as personal accounts) with vast social networks and online communities, sometimes unrelated to Russian political issues.

5.2.2.1 Sociotechnical Model of Target Audience Manipulation[11]

Successful information confrontation is more than the mere dissemination of messages, whether radio broadcasts, posters and billboards or social media posts (i.e., using traditional and new media); rather, and most critically, it is a theoretically grounded process in which the content of the message or narrative is designed to be meaningful to, and also serves to mobilize, a target audience. In other words, the message must serve a sensemaking function (i.e., give meaning to) as well as provide a justification for and – ideally – guidance on how or what actions the recipient of the message should take (i.e., behaviors to be elicited). To accomplish this high degree of resonance with and mobilize the target audience, information confrontation leverages the following eight interrelated and theoretically grounded sociotechnical mechanisms (which I refer to as the *Barrage Model*) [7]:

1) ***Emotional appeal:*** Messages are designed to induce and exploit emotion (such as fear, anger or surprise), which serves to undermine rational thought and encourage malign or ill-conceived action [38]. Although individual susceptibility to emotional appeal varies significantly, an increased state of emotional arousal is generally achieved through the use of messages loaded with provocative language, images, associations or ad hominin attacks [39]. By using highly emotive language in association with a particular issue, an antagonist likely seeks to undermine actor rational decision-making and encourage impulsivity;
2) ***Belief formation:*** Two factors are important to note. First, research in the field of cognitive psychology suggests that people tend to search for and consume information that confirms, rather than challenges or contradicts, one's existing beliefs [40]. In essence, rather than searching for well-grounded and logical explanations, people search for confirmatory information in order to rationalize and justify existing beliefs, and also to ensure consistency and reliability of the beliefs and actions over time [40]. Second, research also indicates that, rather than changing someone's mind, countervailing information actually hardens an individual's commitment to existing beliefs (i.e., ideational entrenchment), or what is commonly referred to as the back-fire effect [41]. In short, antagonists may be able to identify and exploit specific target audiences, in particular those that – when mobilized towards action – can serve short and long-term objectives (e.g., causing internal strife that distract targeted governments);
3) ***Stereotypes and conspiratorial language:*** Studies indicate the use of stereotypes and conspiratorial language and ideas serves as a cognitive heuristic, simplifying and imposing order on an otherwise complex world. In essence, stereotypes and conspiracies assist the adherent by reducing mental effort for recall and decision-making [42], [43], [44]. When combined with calls to action, an antagonist may use conspiracy theories to mobilize communities, specifically against their government or state institutions;
4) ***Filter bubbles:*** In addition to people naturally looking for information confirming existing beliefs, algorithmic and computational models serve a similar function by curating information retrieval based on a user's search history and personal details [45]. As a result of using search engines over time, a user will become increasing informationally isolated, fragmented and marginalized [46], receiving increasingly narrow or restricted bands of information, which most often confirm rather than challenge the user's pre-existing beliefs. By manipulating algorithms and computational models and ensuring specific types of (reinforcing) information are delivered to a target audience, an antagonist may be able to create and exploit specific filter bubbles for political purposes;[12]

[11] This section has been adapted from Lauder, (2020) [7].

[12] It is recognized that more recent scholarly material, particularly by Dahlgren (2021) [47], questions the concept of filter bubbles. However, a discussion of Dalhgren's argument is beyond the remit of the paper.

5) ***Echo chambers:*** The result of filter bubbles and belief formation, echo chambers are digital information environments in which existing beliefs are reinforced and amplified (through algorithms and computational models) that allow people to find psychological comfort by participating in like-minded digital communities [6], [48], [49]. Several scholars have criticized echo chambers for encouraging and creating ideological safe-havens for bias and extremist beliefs and – more generally – for skewing and damaging understanding [6], [48]. As a result, echo chambers represent a pool of potential activists for antagonists and, depending upon their existing political and social beliefs, may be primed for malign influence;

6) ***Ingroup bias:*** This concept is closely associated with filter bubbles, echo chambers and conspiratorial language and can be understood as a pattern of behavior favoring one's group (ingroup) over that of other groups (outgroups) [50]. One of the leading explanations of ingroup bias can be found in *Social Identity Theory*, which proposes that identity-based favoritism, and claims of ingroup exclusivity, is utilized to enhance one's sense of self-importance and efficacy [51]. Critically, antagonist can exploit ingroup bias to mobilize social and political groups and movements, including for the purposes of instigating violence and other extreme behavior against members of outgroups, or social and political structures that are seen as supporting, promoting or protecting the interests of outgroups;

7) ***Information saturation:*** The objective of information saturation to overwhelming the information space with messaging and displacing countervailing information sources. This is typically achieved through a three-pronged approach of message repetition (frequently disseminated), pervasiveness (across multiple means of communication) and persistence (disseminated across prolonged period of time) [6]. Closely associated with confirmation bias, this approach leverages the *illusory truth effect*, which is the tendency to believe false information if repeated [52], [53], [54], [55]. By inundating a target audience, especially those belonging or confined to an informational enclave, an antagonist is not only able to supplant external information sources but may be able to slowly move a target audience towards a new appreciation or understanding of social reality; and,

8) ***Creeping normality:*** Is both a process and the outcome of all the mechanisms working in conjunction. Creeping normality refers phenomenon of a population accepting as normal a major or significant alteration in conditions if that alteration occurred incrementally, through unremarkable and otherwise inconspicuous increments of change [56]. In other words, if the change remains below the threshold of collective awareness, it will be accepted as a natural evolution or course of events [56]. Through this process, and if properly manipulated, an antagonist may reverse significant advancements of a society or, alternatively, push it towards the precipice of collapse, such as through internal strife.

This model also takes into consideration the evolving nature of information confrontation, specifically pre-2016 tactics that focused on the pervasive (i.e., blanket) dissemination of inflammatory, or explicitly pro-Russian, messages with little attention paid to how the messages would resonate with an audience.[13] In fact, early messaging campaigns were mostly about offending or insulting audiences and gaining international media attention (for amplification), irrespective the quality of or the effect generated by the message. However, since 2016, the Russian government and its proxies have engaged in a deliberate and curated approach of message dissemination focusing on establishing deeper and more meaningful audience engagements by building or coopting and exploiting informationally isolated or otherwise marginalized communities, such as political and social activist groups. Central in the Russian government's revised approach to information confrontation is the appearance of *information source authenticity*, specifically that

[13] It should be noted that this is a general/descriptive, rather than prescriptive, model of target audience manipulation. In addition, the development of this model reflects the employment of traditional and new media, as well as other technical and non-technical means of delivery, and across all levels of conflict, and is not specific to the social media. As such, not all components of the model are or need to be utilized in a particular information activity. Rather, specific components are leveraged based upon the nuances and idiosyncrasies of the target audience and the behavioural effect to be generated, as well as the means of message delivery.

the disseminator or organizer (of an online group or event) belongs to the community being targeted. Recognizing that it is difficult to feign authenticity from a nondescript office building in St. Petersburg or Moscow, the Russian government, through its proxies and various cut-outs, have increasingly employed local interlocutors to conduct social media campaigns [18], [57], [58], [59], [60]. This approach not only enhances authenticity but also deniability, essentially adding layers between the Russian government and the influence operatives.

Before proceeding with an examination of the various incidents targeting the Canadian Armed Forces, several key points about information confrontation should be reiterated:

1) Clear lines of responsibility of have been eliminated and state and non-state entities conduct activities across the different forms;
2) Hierarchical control has been replaced by a highly decentralized approach to command and control that is based on expressions of strategic intent from the central administration;
3) Non-state actors no longer serve merely as disseminators, purveyors or the intermediate means of messages but now play an integral role in the design, planning and execution of activities;
4) The combined employment of state and non-state actors provides the Russian government with a number of distinct advantages, including deniability as well as vast reach and penetration of a variety of target audiences;
5) While much of theory and practice is borrowed from or originated during the Cold War, new concepts, organizational structures, and communication technologies have been embraced, essentially establishing a new approach to the planning and execution of information confrontation;
6) Informational confrontation is rarely conducted in isolation and are typically a part of a broader campaign that includes a range of military and non-military measures, and effects against a target can be generated indirectly;
7) Tactics and methods of information confrontation have evolved over the last decade, from broad dissemination of offensive and pro-Russian messaging to mass or undifferentiated audiences to messages tailored to the needs and interests of specific audiences, in particular groups primed for social and political action, including violence; and,
8) Truth is no longer relevant but rather can be created and managed – for specific target audiences – through persistent information engagement.

5.3 INCIDENTS OF RUSSIAN INFORMATION CONFRONTATION

The purpose of this section is to examine a number of incidents in which the Russian government, and/or its proxies, employed information confrontation for the purposes of undermining the credibility of the Canadian Armed Forces and, by extension, NATO, with a particular focus on the missions in Latvia and Ukraine. The overall goal of this section is to identify and briefly discuss the sociotechnical mechanics and – if possible – the effects of the information attacks. Due to space limitation, this section does not offer an exhaustive list of incidents targeting the Canadian Armed Forces; rather, it offers an examination of a handful of exemplary attacks. To put the incidents into context and demonstrate the existence of a broader campaign, this section will highlight a number of other incidents targeting NATO missions, NATO military forces, political leaders, or government institutions in the Baltic states and Ukraine.[14] It is important to note that the employment of information confrontation by the Russian government is not just about undermining the Canadian Armed

[14] It should be noted that, while some links between incidents or examples of information confrontation can be demonstrated, which implies a degree of forethought, design, and planning, it is impossible to identify whether incidents are planned (i.e., created), opportunistic (i.e., exploit an unexpected situation), or reactive. The reason for this is because the perpetrators of information confrontation, whether they are state or non-state actors/proxies, generally do not discuss the why and how of an activity.

Forces; rather, attacking the Canadian Armed Forces is a small part of a much larger and more complex campaign to undermine and fracture NATO, which is a critical step towards destabilizing specific countries in eastern Europe and gaining geopolitical dominance in the region.

5.3.1 Latvia

5.3.1.1 Incident 1: Blue Division

Although it can be argued the Russian government started to target the Canadian Armed Forces well before the actual deployment of troops to Latvia (e.g., smear campaign against Chrystia Freeland and a social media troll campaign targeting Harjit Sajjan, the Minister of Defence), one of the most noteworthy information attacks – and in a way setting the standard – came just days prior to ceremony marking the official start of the Canadian-led, enhanced Forward Presence (eFP) mission at Camp Adazi on 19 June 2017. Largely employing disinformation in which historical truths are leveraged and manipulated for ideological purposes, a pro-Russian blogger published an opinion-editorial (op-ed) article on 14 June 2017 on a popular online Russian-language forum in the Baltic states referring to NATO as a "circus" and dismissing the contributions made by NATO nations (with the exception of the US) as "amusing." The article also equated the mission to occupation of the Baltic region by Germany in World War II and claimed the Spanish armored unit now deployed to Latvia fought as part of the Wehrmacht Blue Division [61]. Clearly designed to elicit an emotional response and undermine the credibility of the eFP mission, the article also references Colonel Russell Williams (a convicted murderer), posting several photos of him dressed in uniform as well as women's underwear, and called him a "true Canadian" [61]. The article did not mention the photos of Williams were presented as evidence by the Crown prosecutor in his criminal case, nor did it indicate he was convicted and sentenced to life imprisonment and stripped of his military rank and awards. However, the article did suggest the photos were gleaned from his social media profile – effectively implying his was still an active member of the Canadian Armed Forces. On the same day, the article, along with the photos of Williams, was posted on *Vesti*, a Russian-language news outlet known for its pro-Kremlin coverage,[15] essentially amplifying the reach of the article to a broader, more mainstream audience.

5.3.1.2 Incident 2: NATO Littering

On 28 September 2017, *Sputnik* (a Russian state-controlled news agency), along with *Press.lv*, *MixNews.lv*, *Focus.lv* and *Regnum.ru* (all Russian-language news portals) published similar articles about a local resident who allegedly discovered garbage left in the woods by soldiers near Camp Adazi [63], [64], [65]. The woman posted a photo of the garbage (which included discarded water bottles, several rusted tin cans and single US military meal pack) on at least two Facebook groups on 26 September 2017 and commented that the soldiers were, "Pigs, not people" [66]. The post immediately garnered several responses critical of NATO, including one person who claimed to have also discovered garbage in the woods left by the military and another person recalling a 2014 brawl involving drunken NATO soldiers [67].

However, the incident was a complete fabrication. In an investigative article written by researchers from Vidzeme University College, the authors determined the items identified in the photo were not actually purchased or used by the Latvian government and that the photo (posted on Facebook and republished on the various news portals) was actually more than a year old and originated from a Russian webpage with no connection to the person who made the Facebook post and the claims of littering soldiers [68].

Simple in design, the information attack – which fused elements of propaganda and disinformation – was conducted in two phases. The first phase involved using a local identity or persona – which offered

[15] *Vesti* is part of a media network, Media Nams Vesti, which operates in Latvia but has a readership from across the Baltic states and Russia. A study of *Vesti's* operations indicate that it has attempted to consolidate Russian-language readership in the region, and that it engages in deceptive techniques, such as manipulating the headlines of republished articles and presenting opinions as facts [62].

authenticity – to make the initial post and complaint about NATO. This phase gained some immediate and local traction, including both negative and positive comments about NATO. The second phase involved the amplification of the story by pro-Kremlin media outlets to enhance the spread of the false story and garner greater national and international attention, in particular amongst Russian-speaking audiences. It should also be noted that the publication of the articles critical of NATO coincided with – and was likely meant to distract from – an official visit by the Defence Ministers of the contributing nations, including the Canadian Minister of National Defence.

5.3.1.3 Incident 3: Riga Housing Shortage

In the summer of 2017, a local real estate company released a trend report on accommodation searches, availability and pricing for Riga. In the report, the real estate company noted both an increase in prices and a reduction in availability and attributed the trend to the posting-in of Canadian soldiers to the NATO mission as well as students securing accommodations for the start of the fall semester. The rather innocuous and factual statement garnered widespread local and international media attention on 11 August 2017, initially by *LETA* and then a number of Latvian-based news agencies (e.g., *MixNews*, *DELFI*, *TVNet*, *LSM.lv*, *BaltNews* and *Gorod*), most of which provided concise and matter-of-fact coverage as well as some positive comments concerning the relationship between soldiers and local residents and landlords [69], [70]. This was followed by articles appearing in the *EAD* (*EurAsia Daily*), *Vesti* and *Sputnik*, all Russian-language publications, which indicated that NATO members were looking for exclusive or high-end accommodations and that the Latvian government was not adequately prepared for the influx of soldiers [71]. The article published by *Vesti* further criticized the Latvian government and called the Prime Minister a "liar" and claimed the government had spent more than 9 million Euros to host the eFP mission, which (according to the article) was paid for by local taxpayers [72].

The incident represents a classic example of disinformation in which a real or actual event or story is leveraged and embellished or manipulated, such as through the addition of an inflammatory or provocative statements or headlines, to shape public opinion.[16] Like many of the other incidents, the information activity is designed to create and reinforce a wedge between the Latvian government and the local population, and to undermine the credibility of the Canadian Armed Forces and NATO, specifically by creating the perception that the military presence is a burden on the economy and taxpayers. In a related incident, this theme was reinforced two weeks later when several pro-Russian news outlets reported the opening of new barracks at Camp Adazi. While some of the articles were fact-based, a number of pro-Russian media outlets published articles critical of the spending, arguing that the Latvian government is "militarizing" with the intention of provoking a conflict with Russia and serving the interests of the military-industrial complex [74]. The article also noted that five schools could have been built for the cost of the military barracks [74]. Another article published in *Regnum* highlighted the cost of infrastructure development and claimed that while the Latvian government has increased defence expenditures the country also suffered from a pervasive economic, health and education crisis, including high mortality rates [75].

5.3.1.4 Incident 4: COVID-19 Infections

On 20 April 2020, *Baltic Voice*, a Russian-language news media outlet operating across the Baltic region, published an article that claimed more than 20 members of the NATO mission in Latvia tested positive with COVID-19, and that most of those infected had recently arrived from Canada. According to the article, concerns about the infections were first raised on social media by the family and friends of the Canadian soldiers [76]. The article also quoted the Canadian commander (using his name and an actual photo of the Canadian commander), who confirmed that 21 Canadian soldiers tested positive. The Canadian commander

[16] It is important to note that Russian information confrontation is scientifically grounded and borrows from Soviet theoretical and conceptual developments in support of active measures and psychological warfare, some which date to the early years of the Russian revolution [22], [23], [73].

also admitted to knowing of the infections for over a month – which suggested that both Canadian and Latvian military leadership deliberately concealed the infections from the Latvian public.

The interview with the Canadian Task Force commander, however, did not happen; rather, it was fabricated. The article, however, did leverage previous – and factual – reporting from a *Baltic News Service* (BNS) article published on 17 April 2020 in which the Lithuanian government released information about isolation precautions and infection rates amongst its military personnel. The article also criticized NATO leadership for not only putting the public at risk but also for blatant hypocrisy; that is, promoting public health restrictions for the local population while troops participated in military exercises [77].

Two days later, an article authored by Edgars Palladis about the infections appeared in *The Duran*, an online sensationalist news outlet operated by a former member of *RT* and known for disseminating far right-wing and pro-Russian propaganda. The article, which linked back to and largely used the text of the article that appeared in the *Baltic Voice* on 20 April, claimed the infection rate amongst NATO members had significantly increased and suggested the infections were not limited to military bases because NATO troops continued to conduct exercises across Latvia and many military members lived in off-base accommodations. The article also pointed out that NATO military activities continued despite Latvia implementing public health measures, including restrictions on social gathering, and argued the military is a "waste of taxpayer money" [78].

Concerned that the rumors and disinformation about the infection rates amongst NATO military members had the potential to create a rift between the Latvian population and the NATO mission, the Latvian government responded to the Palladis article (that appeared in *The Duran*) in two articles and a press release. In the first article, published on 23 April 2020 in *SARGS.LV* (an online popular news publication by the Ministry of Defence), government representatives dismissed the COVID-19 disinformation and claimed Palladis was a false online persona or pseudonym used by a professional pro-Russian agitator [79]. The article also identified numerous errors in the article posted on *The Duran*, including inconsistent information, false quotes and erroneous graphics, and provided an official quote from the Canadian commander who stated the information and (his) quote that was used in the original article were fabricated [80]. In the second article appearing on 25 April, representatives from the Ministry of Defence exposed the (questionable) origin of the author and the myriad of connections of *The Duran* to the Russian government. The article also identified and explained how the original article was a part of an elaborate Russian disinformation operation, and how the author attempted to amplify the fabrication by laundering it through more reputable and well-known writers and online news platforms. Lastly, the article identified how the author had conducted a series of other disinformation activities, such as targeting the 2017 French Presidential election [81]. The press release, which appeared on 27 April on the Ministry of Defence website, restated many of the concerns identified in the *SARG.LV* articles and declared *The Duran* article to be a blatant act of disinformation. The press release also stated *The Duran* had been involved in numerous disinformation activities, including writing erroneous stories about a spoofed email from NATO Secretary General to the Lithuanian government on 21 April 2020 indicating that NATO was immediately shuttering the mission in the country due to concerns about COVID-19 [82].

5.3.2 Ukraine

5.3.2.1 Incident 5: Botched Special Forces Raid

Initially appearing on a Russian blog published by Nikolay Starikov (the leader of a Russian political party) on 06 August 2016, a relatively detailed article, citing an unnamed source, was published that claimed approximately 11 Canadian Special Operations Forces (SOF) members were killed in a failed raid on Russian separatist forces along the line of demarcation in the Luhansk region of eastern Ukraine on 23 July 2016 [83]. According to the article, the Canadian SOF team arrived in the area on 22 July 2016 (a day prior to the alleged raid) and attempted to conduct a tactical demonstration to Ukrainian military observers when

they were discovered and engaged by Russian separatists. The article further stated the deceased Canadian military personnel were retrieved and flown back to Canada on 26 July 2016. The article was republished the same day on *Politikus.ru*, a Russian-language news portal, and reappeared in several Russian blogs and pro-Kremlin news sites, including *Stalker Zone* (which is an English-language advocacy journalism site known for publishing Russian propaganda and disinformation) in early September 2016 [84], [85], [86].

To the casual reader, the story probably seemed true, especially since the article contained a sufficient amount of detail (e.g., the type, structure and size of force, as well as names of key Ukrainian and Canadian military personnel involved in the incident). However, to a more informed or knowledgeable reader, the story was amiss. For example, the article suggested the raid was coordinated by the Canadian Security Intelligence Service (CSIS) along with the Canadian Defence Attaché to Ukraine. Another oddity is that it was claimed in the article that the Canadian SOF team was a part of a CSIS-led operation in Ukraine but assigned to the Ukrainian Ministry of Health, and that the attachment was personally approved by the Prime Minister of Canada during a recent state visit to Ukraine. In reality, neither CSIS (which does not conduct foreign operations) nor the defence attaché would be involved in the planning and execution of military operations. Moreover, the Prime Minister does not personally allocate or approve military resources.

5.3.2.2 Incident 6: Mine Strike

On 17 May 2018, the website of the armed forces of the Dontesk People's Republic (DPR) published a press release that claimed the Ukrainian military engaged in an act of provocation by fabricating a situation along the line of demarcation near Avdiivka (a small town just north of Donetsk) that resulted in the deaths of or injury to several NATO military personnel [87]. The press release indicated that Ukrainian military commanders "deliberately brought guests" (i.e., foreign military personnel) into a minefield which resulted in the deaths of three Canadian military personnel and injured several US and Ukrainian military observers. The press release further noted that the purpose of the provocation was for Ukrainian authorities to blame DPR armed forces for the attack and to use the incident to advocate for and justify military intervention by NATO.

Similar to the false report of Canadian military deaths in 2016, the press release was republished and generated significant discussion on numerous pro-Russian blogs, social media accounts and news sites. Of note, the press release also originated from an official and trusted – at least from the perspective of pro-Russian supporters and information consumers – source and contained enough detail (e.g., location of the incident, types of units involved, number and nationality of casualties, etc.) to make the incident appear as though it actually happened. However, where the previous incident received limited coverage (i.e., limited to Russian blogs and fringe news media), the mine strike incident gained both Ukrainian and international media coverage, including mainstream Canadian news networks [88], [89], [90]. Although international media coverage quickly declared the incident 'fake news,' the virality of the story necessitated a response form the Canadian government, which assuaged the concerns of Canadians and denounced the report as propaganda.

5.3.2.3 Incident 7: Freeland Smear Campaign

Although largely occurring in Canada – or at least the majority of the effort appears to have been executed in Canada – the smear campaign conducted against Chrystia Freeland was arguably designed to undermine the credibility of the Canadian government as well as the Canadian Armed Forces presence in Eastern Europe, primarily Ukraine but also Latvia. Literally launched the same day that Freeland was appointed as the Minister of Foreign Affairs [91], the smear campaign started with a series of posts on a pro-Russian social media account, seemingly located in Canada, on 10 January 2017 that cited documents from the archives of the Alberta government about Freeland's grandfather, Michael Chomiak, and accused her of being sympathetic to Nazism.

The following day, an editor from *VICE* magazine, who was conducting an interview on an unrelated matter at the Russian embassy in Ottawa, was handed a dossier from an unidentified embassy staff member detailing Freeland's grandfather's interaction with the German military in occupied Ukraine during World War II [92], [93]. Similar to the previous day's social media posts, the dossier was based on publicly available information held in the archives of the government of Alberta.

A week later, on 19 January 2017, a lengthy and detailed article written by John Helmer appeared on his blog, *Dances with Bears,* and also in the *Russia Insider,* a pro-Russian newspaper believed to be funded by Konstantin Malofeev (a Russian oligarch close to Putin and accused of having funded pro-Russian separatists in Ukraine and the attempted coup in Montenegro), as well as other pro-Russian social media sites [94], [95], [96]. Seemingly based on archival documents, the article claimed Freeland lied about her grandfather's interaction with the German army during WWII and stated she was actively "preaching race hatred of Russians" [97]. A former White House aide, Helmer, who moved to Moscow in 1989, is reputed to have been an agent for the KGB [98].[17]

Between 19 and 26 January 2017, more than 30 different pro-Russian Twitter accounts posted or re-tweeted the claims regarding Freeland's grandfather or linked to and promoted the Helmer article [99].[18] Many of the social media accounts, some of which had thousands of followers, were known Russian social media trolls belonging to or affiliated with the IRA. On 27 January 2017, a computer-generated audio recording reciting the text of Helmer's article was posted to YouTube as well as several other social media platforms. The Helmer article was published by the *Strategic Culture Foundation*, a Russian thinktank and online journal operated by the SVR and the Ministry of Foreign Affairs and a known outlet of Russian propaganda and disinformation [97], [100], [101]. Within a week, the story of Freeland's grandfather, and accusations that Freeland was sympathetic to Nazism, went viral across several social media platforms.

Just over a week later, Stanislav Balcerac, a Polish journalist known to support right-wing political movements, published an article in the *Warszanka Gazeta* (Warsaw Gazette), a weekly publication known to publish hate-based and anti-Semitic articles [98], [102]. The same article is also published in *Polska Bez Censury* (Poland Without Censorship). Later in February, Arina Tsukanova, a pro-Russian journalist allegedly based in Crimea (Global Engagement Centre, 2020), published an article in *Consortium News*, a US-based independent, online news service [103].[19] Although *Consortium News* sued a Canadian news network for claiming it was part of an elaborate Russian cyber-influence campaign [105], Tsukanova was subsequently reported to be a sock puppet (i.e., a fictitious persona) operating for the Russian foreign intelligence service through the *Strategic Culture Foundation* [100], [106].

During a press conference on 06 March 2017 to announce an extension to Operation UNIFIER, the Canadian military training mission to Ukraine, a reporter asked Freeland about Russian media outlets and websites and claims her grandfather was a Nazi collaborator. In response, Freeland stated that Russian disinformation and other smear campaigns, similar to those that recently occurred in the US and Europe, should be expected. However, the question of her grandfather's role during WWII at the press conference, which was covered by several Canadian national news media agencies, served not only to push the story into the mainstream but also provided an opportunity for the Russian government – through Kirill Kalinin, the

[17] As noted by Ledeneva [73], smear campaigns are based on political (e.g., abuse of power, disloyalty or incompetence, etc.), economic (e.g., embezzlement, nepotism, etc.), criminal (e.g., links to organized crime or bribery, etc.) and/or private information that compromising the target's reputation, including but not limited to the misdeeds, illegal or unethical behaviour of family members, or unpopular personal beliefs or behaviours. Ledeneva also points out that a sustained and serious campaign against a target will draw from information from across all four categories and that some of the most effective smear campaigns are not based on perceived or real illegal behaviour but related to private life and behaviour associated with or contravening strong social norms or values.

[18] The initiation and propagation of the smear campaign against Freeland was identified and reported on by the EU East StratCom Task Force on 26 January 2017 [99].

[19] *Consortium News* was edited by Robert Parry and is regarded by Media Bias/Fact Check website to be a left leaning but with mixed reliability/mostly factual (Media Bias/Fact Check, n.d.) [104].

press secretary of the Russian embassy in Ottawa – to publicly criticize Freeland and question her credibility [107]. The story of Freeland's grandfather's role in WWII, and Freeland's warning of Russian disinformation, effectively dominated news media reporting and overshadowed the announcement of Canada's renewed commitment to the NATO mission in Ukraine, which was likely the objective of the Russian disinformation campaign [93], [98].

However, that was not the end of the smear campaign. On 21 March 2017 and leveraging the story of Freeland's grandfather and accusing her of lacking integrity and engaging in anti-Russian bias, the Russian Congress of Canada lodge a formal complaint with the Prime Minister. In addition to making spurious claims that Freeland lacked the proper qualifications for the job (as Minister of Foreign Affairs), the letter implied a connection between her grandfather's role in WWII to her support for Ukrainian exiles and related political issues, suggesting she acquired pro-fascist sympathies from her grandfather [108].

While initially generating significant news media attention and public interest in Canada and abroad, as well as generating some negative coverage, some of which called into question the veracity of claims the incident was an act of Russian disinformation [109], the smear campaign was and is still used in Russian information confrontation, especially those designed to shape the opinions of Russian linguistic audiences in eastern Europe [93]. In addition, the smear campaign is often referenced in other disinformation activities designed to undermine Ukrainian political support abroad, in particular in Canada [110].

In response to the smear campaign, and also prompted by the attempted assassination of Sergei Skripal in the United Kingdom by GRU agents, the Canadian government announced the expulsion of four Russian diplomats in March 2018. The diplomats, who were based in Ottawa and Montreal and included Kalinin (who was alleged to have orchestrated the smear campaign by sending information about Freeland's grandfather to various news agencies), were identified as intelligence officers and alleged to have interfered in the operation of democratic institutions, including to have engaged in a campaign to shape Canadian public opinion [111], [112], [113]. Three of the four were also identified as having conducted cyber-influence activities while based at the Russian consulate in Montreal, specifically an effort designed to discredit the World Anti-Doping Agency (WADA) and spread other disinformation related to Canadian institutions [114].

5.3.2.4 Other Incidents

While this report is not meant to be a comprehensive study of Russian information confrontation, it is important to note that these activities are rarely conducted in isolation. Moreover, information confrontation targeting other NATO countries, such as US or German forces deployed to Lithuania, may negatively impact the Canadian missions, as target audiences do not often differentiate between the various NATO forces. As a result, incidents targeting other NATO forces and allied governments in Eastern Europe should also be taken into consideration. Some of these informational attacks include, but are not limited to, the following:

1) **16 October 2016:** Russian state news media claimed that mercenaries from Canada and other NATO countries had taken up positions along the line of demarcation in eastern Ukraine and were training Ukrainian soldiers in sniper and sabotage skills [115];
2) **21 December 2016:** In a public statement, Alexander Darchiev, Russia's ambassador to Canada, claimed the upcoming deployment of Canadian troops to Latvia is a waste of resources and a distraction to the "real threat" of international terrorism. Darchiev also called upon Canada to be an honest broker and distance itself from US foreign policy, as it did during the Iraq War [116];
3) **February-March 2017:** A smear campaign targeting Harjit Sajjan, Minister of Defence, is conducted in the lead up to the Latvian mission in which his appearance (i.e., wearing a turban) was made a focal point and criticized [117];

4) **March 2017:** Pro-Russian news media operating in Latvia reported that Latvian defence officials secretly amended an agreement to allow NATO soldiers to carry loaded weapons in the country [118];
5) **20 May 2017:** A Russian news media outlet published a story about three separate vehicle accidents involving NATO personnel. While the article did not provide details as to the causes of the accidents, the article employed a provocative title that implied the NATO members were likely under the influence of alcohol [119];
6) **25 May 2017:** A Russian news media outlet published a story about an upset Estonian resident who fired warning shots at NATO troops participating in an exercise in his town. The article also mentioned several other incidents involving NATO personnel during the exercise, including traffic accidents and personal injuries. The article also asserted local residents were tired of the military exercises and that Estonia was not prepared to host the eFP mission [120];
7) **June 2017:** Shortly after the official start of the enhanced Forward Presence mission in Latvia, a number of fake accounts (of a senior Canadian military officer) were created on Twitter and attempted to build a community of followers;
8) **04 June 2017:** Russian news media outlets reported an incident in which four intoxicated German soldiers got into a fight and were sent to a local hospital with unspecified injuries. The article also mentioned the NATO soldiers received mandatory training on proper behavior prior to deploying on the NATO mission and suggested the soldiers ignored the training [121];
9) **20 June 2017:** Russian news media outlets reported that an unknown number of local women had been raped by deployed NATO soldiers and that the incidents were covered-up by Latvian authorities. The article also claimed that local authorities dismissed the claims of rape as a Russian provocation [122];
10) **21 June 2017:** A Russian news media outlet reported an incident of vandalism in Lithuania involving a NATO soldier. The article claimed the soldier was "lectured" and fined 15 Euros after he was caught urinating on a government building. The article also mentioned several other incidents of wrongdoing involving NATO personnel, including German soldiers involved in a "drunken fight" and numerous vehicle accidents [123];
11) **01 July 2017:** Russian news media outlets reported that Lithuanian residents were upset at the deployment of NATO troops and claimed that some residents were frightened by the presence of the military while others had been attacked or assaulted by NATO soldiers [124];
12) **02 July 2017:** Russian news media reported an incident in which four intoxicated members of the Netherlands military started a fight in a Vilnius restaurant which resulted in a single victim being sent to hospital for treatment. The article also mentioned a number of previously reported incidents involving drunken NATO soldiers or vehicle accidents [125].
13) **24 August 2017:** A pro-Russian, English-language news website published an article that claimed the US military had set up a network of biological warfare labs in Ukraine, effectively turning the country into a "proving ground for a new generation of US biological weapons" [126];
14) **18 October 2017:** A pro-Russian news media outlet in Latvia published a story that claimed the NATO presence is demeaning to the local population. The article also summarized a number of claims previously made in pro-Russian media about misconduct by NATO soldiers, such as bar fights, littering, acts of vandalism, and vehicle accidents. The article also claimed that the offending soldiers are quickly and secretly removed from the Baltic region to avoid criminal prosecution [127];
15) **August – September 2017:** A significant portion of Latvia's cellphone network in the western portion of the country was disabled by Russian military electronic jamming on 30 August. On 13 September, another electronic attack effectively knocked-out Latvia's emergency telephone service [128], [129];

16) **18 January 2018:** Russian operatives hacked the website of a popular Lithuanian TV channel and inserted a fake story about the Minister of Defence and claimed he was gay and that he had been accused of sexual harassment [130]. At the same time an email, which referenced the story but also had attachments that contained malicious code to facilitate espionage and data retrieval, was sent to Lithuanian government agencies, news media outlets and politicians [131];

17) **07 June 2018:** *The Baltic Course*, an online news website service in the Baltic region is hacked and a fake story is posted claiming a child riding a bicycle was killed by a US armored vehicle during a military exercise [132]. The fake article, which was purported to be from a mainstream Lithuanian news provider and leveraged news about a real vehicle accident involving US armored vehicles, provided details of the incident, including the name of the US military unit involved, a false statement from a Lithuanian military Public Affairs Officer, and a manipulated photograph of a mangled bicycle near a US armored vehicle. The story was also reposted to several Russian-language blogs (Staff Writer, 2017d). Website administrators for *The Baltic Course* were made aware of the hack and published a correction, identifying the original post as a fabricated news story [133];

18) **March 2019:** Pro-Russian news media in eastern Ukraine reported that US military personnel with Russian language skills were recruited and provided with Ukrainian passports, which they used to infiltrate Russia, ostensibly to conduct acts of sabotage [134];

19) **November 2019:** Although the objective of the letters is uncertain, a German-based self-publishing website is utilized by Russian operatives to post two forged letters bearing the signature of Janis Sarts, the director of the NATO Stratcom COE in Latvia. The letters claimed the center was allocated funds to establish a new cyber unit to block access to online content, specifically Russian media criticizing NATO activities [135];

20) **20 June 2019:** The content management systems of several news websites in Lithuania and Latvia are hacked and fake stories posted that claimed NATO forces conducting an exercise in Lithuania accidentally contaminated the Neris River with depleted uranium munitions [136].

21) **September 2019:** A popular, international petition website is leveraged to disseminate fabricated claims of German troops desecrating a Jewish cemetery in Lithuania [137], [138];

22) **18 October 2019:** A fake press release from the Lithuanian MFA that claimed the US planned to move nuclear weapons from Turkey to Lithuania was released on social media and subsequently reported on by several legitimate news media outlets [139];

23) **19 December 2019:** The content management system of a leading news outlet in the Baltic states is hacked and a fabricated article claiming Lithuanian police arrested two US Army sergeants in connection to a violent carjacking is posted. The fake article named two US Army personnel involved and identified the unit to which they belonged. The fake article, which stated the individuals could not be charged due to an agreement between the US and Lithuanian governments, also used the name of a well-known author of defence-related articles (in the byline) [140]; and,

24) **23 March 2020:** *New Russia*, a pro-Russian online news website operating in eastern Ukraine, reposted a summary from *FAN* (a news agency linked to Yevgeny Prigozhin, a close associate of Putin) doxed[20] two Canadian military intelligence officers operating in Ukraine [141].

Additional incidents include a series of enduring and often inconspicuous technical attacks occurring throughout 2017 in which the cell phones of NATO soldiers deployed on eFP in the Baltic states were targeted, including attempted hacks of personal social media accounts [142], [143]. It is believed that the attempted hacks were conducted by Russian electronic warfare units using mobile and portable devices as

[20] Doxing is the publication or posting of private or personal information about an individual, typically as a form of intimidation.

well as Unmanned Aerial Vehicles (UAVs) and conducted for the purposes of intelligence collection and intimidation [144]. Although not directly related to NATO but designed to undermine democratic institutions more broadly in Central and Eastern Europe, hackers working on behalf of or associated with Russian intelligence services conducted a series of cyber-attacks between 2018 and 2019 targeting embassies as well as academic institutions, news media outlets and journalists, private businesses, and non-government organizations and government agencies in Ukraine [145], [146], [147]. Additionally, a GRU cyber team conducted a campaign in August 2020 in which they embedded a hard-to-detect malicious payload, likely to facilitate clandestine data extraction, that impersonated photo files in fake NATO training documents, which was sent to Azerbaijan and other NATO partners and institutions [148]. The purpose of these campaigns was to slowly undermine the reputation of and subtly discredit NATO, specifically in Central and Eastern Europe.

5.3.3 Observations

Based on these incidents of Russian information confrontation, several observations can be made:

1) Attacking the reputation of and attempting to undermine and disrupt the Canadian Armed Forces – and by extension NATO – does not require direct and explicit confrontation (e.g., targeting Canadian military personnel on the mission) but can also be conducted indirectly, such as targeting political leaders, investigative journalists, commercial entities or manipulating targeting audience perceptions in Canada;
2) Information confrontation is rarely about achieving a knock-out blow or a decisive strike and more about slowly chipping-away at and undermining the foundation of credibility of the target and gradually shifting the perspective/attitude of a target audience. The idea is that this form of indirect and enduring upstream engagement will ultimately change how the target audience views the target and facilitate downstream political and policy changes that support Russian geopolitical objectives;
3) Ambiguity, deniability, and decentralization continue to play a key role in the design and execution of information confrontation, which is largely achieved through the employment of proxies and other information intermediaries, such as pro-Kremlin news media outlets. The maximal use of decentralization and proxies for the purposes of enabling psychological effects through information diffusion (dissemination through interaction) represents a position of strength for the Russian government;
4) Information confrontation includes both technological and non-technological means, including social media. While electronic warfare and cyber capabilities have been employed to facilitate attacks, such as hacking content management systems, email spoofing or embedding malicious code in attachments, these appear to be used sparingly, possibly because of cost and the degree of skills required to facilitate the information attacks; and,
5) Most information attacks leverage real or actual information or draw upon local social or political issues or generally held beliefs/local reasoning, which are then embellished or manipulated in to maximize impact on a target audience. This anchoring in reality is done to enhance believability (of the message) but also to make denials (on part of the target) more difficult. While wholesale fabrications do occur, these incidents tend to be rare or in the minority. Moreover, even information confrontation failures (e.g., incidents that do not gain significant traction or have been rebutted) can be leveraged in or by future attacks as if they are records of true events.

5.4 CONCLUSION

The full-scale invasion of Ukraine by Russia on 24 February 2022 invalidated many assumptions about Russia's use of its military instrument of power. However, it should be expected that Russian use of information confrontation will remain consistent, and that much of the competition with Russia will occur in

the information environment, specifically through an enduring, pervasive, and largely covert campaign focused on social and political subversion, including the fracturing of the relationship between host or member countries and NATO. Based upon an examination of numerous examples of information confrontation targeting the Canadian Armed Forces and other NATO forces and assets in the Baltic states and Ukraine and drawing upon other studies of Russian political warfare conducted by DRDC between 2014 and 2020, two key implications and recommendations for response have been identified.

First, and while multifaceted informational attacks (i.e., combining multiple means of dissemination, such as hacking news media websites and platforms to post fake articles and replicating the story across social media and blogs or disseminating a fake document with embedded malware) have occurred, they remain relatively rare. Rather, Russian information confrontation tends to be one dimensional in nature, albeit high frequency (i.e., lots of attacks using a single means of content or message delivery). This is likely due to the decentralized nature of the Russian information confrontation, but also because multifaceted and complex attacks, using multiple or technical means, requires additional expertise and resources, which may not be readily available – especially to proxies. As a result, the Canadian Armed Forces and NATO should expect the Russian government to continue to employ quick, easy and relatively simple informational attacks, at least for the foreseeable future. That being said, neither the Canadian Armed Forces nor NATO should be complacent to or dismissive of these informational attacks because they appear simple or mundane, as they tend to have a high degree of resonance with target audiences and contribute to an aggregated effect. Moreover, the Canadian Armed Forces and NATO should develop and maintain structures, processes and capabilities to continually monitor the information environment, gauge audience sentiment/reaction and be positioned to quickly respond to incidents.

Second, while the theoretical underpinnings of Russian information confrontation can be found in Soviet information warfare, it is an evolving capability. As such, the Russian government, and its proxies, have been quick to embrace and integrate new technology but also adapt existing or develop new Techniques, Tactics and Procedures (TTPs) of audience engagement and manipulation (i.e., perception management). One of the key transformations in TTPs has been a shift from highly belligerent and combative messaging, often with an explicit pro-Russian sentiment, largely directed towards unsupportive (e.g., pro-NATO or Western) audiences but broadcasted broadly to messages with a more complaisant and deferential tone delivered to specific target audiences, often by exploiting political and social predispositions and proclivities facilitated via technical means (e.g., filter bubbles and echo chambers) [149]. In other words, there has been a shift from alienating target audiences towards building and maintaining interest-based communities and affinity groups that can be mobilized and exploited in support of Russian geopolitical objectives. Moreover, while most of this tailored audience engagement occurs via online news services and discussion groups, there are indications that Russian influence operatives now utilize Peer-to-Peer (P2P) networks to engage specific target audiences, community segments or digital enclaves. The potential for broad influence via P2P networks is significant, especially when augmented by advanced microtargeting techniques and artificial intelligence – which permits an instigator of an influence campaign to develop user-specific messages, tailored to individual behavioral and psychological characteristics, but employed on an industrial scale [150] Looking out 10 – 15 years, this technology will likely be combined with virtual reality and immersive technology, which will enhance the user-experience by making the interaction highly personal and, therefore, more effective. As a result, the Canadian Armed Forces and NATO should look and prepare to move beyond approaches or tactics that are defined by web 1.0 and 2.0 technologies, including conventional social media (e.g., Facebook, Twitter, VK, Odnoklassniki, etc.) and lean forward and develop means and tools to identify, monitor (for indications of Russian information confrontation and effects generation) and engage decentralized P2P networks and related cross platform chat applications (e.g., WhatsApp, Kik, Telegram, Signal, Viber, etc.), some of which provide end-to-end encryption and anonymous functionality.

5.5 REFERENCES

[1] Kabanenko, I. "Russian Naval Exercises in the Sea of Azov: A Prelude to 'Hybrid'-Style Invasion? Eurasia Daily Monitor, 15(78), 2018. Accessed: March 15, 2021, from https://jamestown.org/program/russian-naval-exercises-in-sea-of-azov-a-prelude-to-hybrid-style-invasion/

[2] MacKinnon, M. "With Russian Troops Amassing on Ukraine Border, an Awful Sense of deja-vu: Is Putin on Cusp of Invasion?" The Globe and Mail, 9 April 2021, https://www.theglobeandmail.com/world/article-ukrainian-commander-sees-parallels-with-2014-as-russian-military-build/

[3] Shlapak, D.A. and Johnson, M. "Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defence of the Baltics. RAND, 2016. https://www.rand.org/pubs/research_reports/RR1253.html

[4] Jonsson, O. and Seely, R. "Russian Full-Spectrum Conflict: An Appraisal after Ukraine." The Journal of Slavic Military Studies, 28(1), 2015, pp. 1-22. https://doi.org/10.1080/13518046.2015.998118

[5] Kagan, F.W. The New Russian Offensive is Intended to Project Power it Cannot Sustain." Time, 6 June 2022. Accessed: July 04, 2022, from https://time.com/6184437/ukraine-russian-offensive/

[6] Lauder, M.A. "Masters of Chaos: The Application of Political Warfare by the Russian Federation in the Contemporary Operating Environment." [DRDC-RRDC-2018-L118]. Defence Research and Development Canada, 2018a.

[7] Lauder, M.A. "Typhon's Song: Examining Russia's Employment of COVID-19 Disinformation to Generate Disruptive Effects." Small Wars Journal, 2020. Accessed: March 15, 2021, from https://smallwarsjournal.com/jrnl/art/Typhons-song-examining-russias-employment-covid-19-disinformation-generate-disruptive

[8] Lauder, M.A., Waldman, S. and McInnis, J. "Curating Dystopia: Russia's Application of Political Warfare and Structural Subversion in the Baltic States and Black Sea Region." [DRDC-RDDC-2020-D021]. Defence Research & Development Canada, 2020.

[9] Lauder, M.A. "Gunshots by Computers: An Examination of Russian Information Confrontation in Doctrine, Theory and Practice." [DRDC-RDDC-2019-D037]. Defence Research and Development Canada, 2019a.

[10] Shelbourne, M. "NORAD: Russians Stay in Airspace 'For Hours' During Flight Operations Near Alaska. USNI News, 31 March 2021. https://news.usni.org/2021/03/31/northcom-russians-stay-in-airspace-for-hours-during-flight-operations-near-alaska

[11] Seddon, M., Foy, H., and Olearchyk, R. "Russian Brinksmanship Leaves Clear Message for Ukraine and Allies." Financial Times, 23 April 2021. https://www.ft.com/content/65e2bdb6-6c1d-4033-b677-a07bb34716ae

[12] Jonnson, O. The Russian Understanding of War: Blurring the Lines Between War and Peace. Georgetown University Press, 2019.

[13] Adamsky, D. The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution of Military Affairs in Russia, the US and Israel. Stanford University Press, 2010.

[14] Renz, B. Russia's Military Revival. Polity Press, 2018.

[15] Bērziņš, J. "Not 'Hybrid' but New Generation Warfare." In G.E. Howard and M. Czekaj (Eds.). Russia's Military Strategy and Doctrine. Jamestown Foundation, 2019. https://jamestown.org/product/russias-military-strategy-and-doctrine/

[16] Hostage, G.M. and Broadwell, L.R. "Resilient Command and Control: The Need for Distributed Control." Joint Force Quarterly, 74(3), 38-43, 2014. Accessed: March 15, 2021, from https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-74/jfq-74_38-43_Hostage

[17] Lauder, M.A. " 'Wolves of the Russian Spring:' An Examination of the Night Wolves as a Proxy for the Russian Government." Canadian Military Journal, 18(3), 2018b. Accessed: March 15, 2021, from http://www.journal.forces.gc.ca/vol18/no3/PDF/CMJ183Ep5.pdf

[18] Lauder, M.A. "Limits of Control: Examining the Employment of Proxies by the Russian Federation in Political Warfare." Journal of Future Conflict, 1 2019b. Accessed: March 15, 2021, from https://www.queensu.ca/psychology/sites/webpublish.queensu.ca.psycwww/files/files/Journal%20of%20Future%20Conflict/Issue%201%20Fall%202019/Matthew_Lauder-Limits_of_Control-Examining_the_Employment_of_Proxies_by_the_Russian_Federation_in_Political_Warfare.pdf

[19] Sabbagh, D. "Only 10% of Russian Spy Operations in Europe Uncovered, Says Former MI6 Chief. The Guardian, 19 April 2021. https://www.theguardian.com/world/2021/apr/19/uk-government-registration-scheme-foreign-spies-boris-johnson

[20] Grozev, C., van Huis, P., and Tsalov, Y. "How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine." Bellingcat, 26 April 2021. https://www.bellingcat.com/news/uk-and-europe/2021/04/26/how-gru-sabotage-and-assassination-operations-in-czechia-and-bulgaria-sought-to-undermine-ukraine/

[21] Robert Lansing Institute. "Russia Uses the Czech Republic to Conduct Destabilization Activities Against the EU and NATO." 2021. https://lansinginstitute.org/2021/04/24/russia-uses-the-czech-republic-to-conduct-destabilizing-activities-against-the-eu-and-nato/

[22] Lauder, M.A. "Truth is the First Casualty of War: A Brief Examination of Russian Informational Conflict During the 2014 Crisis in Ukraine." [DRDC-RDDC-2014-L262]. Defence Research and Development Canada, 2014.

[23] McCauley, K.N. "Russian Influence Campaigns Against the West: From the Cold War to Putin. CreateSpace, 2016.

[24] McIntyre, L. Post-Truth. MIT Press, 2018.

[25] Government of Russia. "National Security Concept of the Russian Federation." 2000a. https://www.mid.ru/en/web/guest/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768

[26] Government of Russia. "On Approval of the Military Doctrine of the Russian Federation." 2000b. http://kremlin.ru/acts/bank/15386

[27] Government of Russia. "The Foreign Policy Concept of the Russian Federation." 2000c. https://fas.org/nuke/guide/russia/doctrine/econcept.htm

[28] Government of Russia. "Information Security Doctrine of the Russian Federation." 2000d. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf

[29] Government of Russia. "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space." 2011. http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle

[30] Government of Russia. "The Military Doctrine of the Russian Federation." 2015a. https://rusemb.org.uk/press/2029

[31] Pynnoniemi, K. "Russia's National Security Strategy: Analysis and Conceptual Evolution." The Journal of Slavic Military Studies, 31(2), 2018. Accessed: March 15, 2021, from https://doi.org/10.1080/13518046.2018.1451091

[32] Ruiz, M.M. "A Shift in Doctrine." Diplomaatia, 168, August 2017. Accessed: 15 March 2021 from https://www.diplomaatia.ee/en/article/a-shift-in-russian-doctrine/.

[33] Government of Russia. "Russian National Security Strategy. Government of the Russian Federation." 2015b. http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf

[34] Government of Russia. "Foreign Policy Concept of the Russian Federation. Government of the Russian Federation." 2016a. http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248

[35] Government of Russia. "Doctrine of Information Security of the Russian Federation. Government of the Russian Federation." 05 December 2016b. http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

[36] Clark, M. "The Russian Military's Lessons Learned in Syria. Institute for the Study of War." 2021. http://www.understandingwar.org/report/russian-military%E2%80%99s-lessons-learned-syria

[37] Lauder, M.A. 2016 "When Lies Become Truth: A Brief Examination of Smear Campaigns as a Key Tactic of Russian Informational Conflict." [DRDC-RDDC-2016-L395], 2016. Defence Research and Development Canada.

[38] Gross, J. and Levenson, R. "Emotion Elicitation Using Films. Journal of Cognition and Emotion". 9(1), pp. 87-108, 1995. https://pdfs.semanticscholar.org/8d06/090b74b1cd4c54bc6c149507bfda6533f80f.pdf

[39] MacFarquhar, N. "A Powerful Russian Weapon: The Spread of False Stories." The New York Times, 28 August 2016. https://www.nytimes.com/2016/08/29/world/europe/russia-swedendisinformation.html

[40] Grayling, A. "Psychology: How We Form Beliefs." Nature 474, 23 June 2011.

[41] Shermer, M. "The Believing Brain: Why Science Is the Only Way Out of Belief-Dependent Realism." Scientific American, 1 July 2011. https://www.scientificamerican.com/article/the-believing-brain/

[42] Tolz, V. and Chatterje-Doody, P. "Four Things You Need to Know About Russian Media Manipulation Strategies." The Conversation, 5 April 2018. https://theconversation.com/four-things-you-need-to-know-about-russian-media-manipulation-strategies-94307

[43] Rudman, L. and Glick, P. The Social Psychology of Gender: How Power and Intimacy Shape Gender Relations. New York: The Guildford Press, 2008.

[44] Uscinski, J. and Enders, A.M. "The Coronavirus Conspiracy Boom." The Atlantic, 30 April 2020. https://www.theatlantic.com/health/archive/2020/04/what-can-coronavirus-tell-us-about-conspiracy-theories/610894/

[45] Bakshy, E., Messing, S. and Adamic, L. "Exposure to Ideologically Divisive News and Opinion on Facebook." Science. 348(6239), 2015. http://science.sciencemag.org/content/348/6239/1130#BIBL

[46] Hosanagar, K. "Blame the Echo Chamber on Facebook: But Blame Yourself, Too." Wired, 25 November 2016. https://www.wired.com/2016/11/facebook-echo-chamber/

[47] Dahlgren, P. "A Critical Review of Filter Bubbles and Comparison with Selective Exposure." Nordicom Review, 44(1), 2022. https://sciendo.com/article/10.2478/nor-2021-0002

[48] Grimes, D. "Echo Chambers Are Dangerous – We Must Try to Break Free of Our Online Bubbles." The Guardian, 4 December 2017. https://www.theguardian.com/science/blog/2017/dec/04/echo-chambers-are-dangerous-we-must-try-to-break-free-of-our-online-bubbles

[49] Hoggan, J. "How Propaganda (Actually) Works." Huffington Post, 31 March 2016. https://www.huffingtonpost.com/james-hoggan/how-propaganda-actually-w_b_9584138.html

[50] Tajfel, H., and Turner, J. "An Integrative Theory of Intergroup Conflict." In M.A. Hogg and D. Abrams (Eds.), Key Readings in Social Psychology. Intergroup Relations: Essential Readings, pp. 94-109, 2001. Psychology Press.

[51] Tajfel, H., and Turner, J.C. "The Social Identity Theory of Intergroup Behavior." In J.T. Jost and J. Sidanius (Eds.), Key Readings in Social Psychology. Political Psychology: Key Readings. Psychology Press, pp. 276-293, 2004. https://doi.org/10.4324/9780203505984-16

[52] Weiss, R. "Repetition of Persuasion." Psychological Reports 25(2), 1969. https://doi.org/10.2466%2Fpr0.1969.25.2.669

[53] Clifton, D. "A Chilling Theory on Trump's Nonstop Lies: His Duplicity Bear a Disturbing Resemblance to Putin-Style Propaganda." Mother Jones, 3 August 2017. https://www.motherjones.com/politics/2017/08/trump-nonstop-lies

[54] Paul, C. and Matthews, M. "The Russian "Firehose of Falsehood" Propaganda Model." RAND, 2016. https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf

[55] Fazio, L.K., Payne, B.K. Brashier, N.M. and Marsh, E.J. "Knowledge Does Not Protect Against Illusory Truth." Journal of Experimental Psychology. 144(5)., 2015. https://doi.apa.org/doiLanding?doi=10.1037%2Fxge000009

[56] Diamond, J. Collapse: How Societies Choose to Fail or Succeed (revised). Penguin Books, 2011.

[57] Alba, D. "How Russia's Troll Farm is Changing Tactics Before the Fall Election." The New York Times, 29 March 2020. https://www.nytimes.com/2020/03/29/technology/russia-troll-farm-election.html

[58] Lister, T., Shukla, S., and Elbagir, N. "Fake News and Public Executions: Documents Show a Russian Company's Plan for Quelling Protests in Sudan." CNN, 25 April 2019. https://edition.cnn.com/2019/04/25/africa/russia-sudan-minvest-plan-to-quell-protests-intl/index.html?no-st=1556190353

[59] Alba, D. and Frenkel, S. "Russia Tests New Disinformation Tactics in Africa to Expand Influence." The New York Times, 30 October 2019. https://www.nytimes.com/2019/10/30/technology/russia-facebook-disinformation-africa.html

[60] Grossman, S. "Russia Wants More Influence in Africa: It's Using Disinformation to Get There." The Washington Post, 3 December 2019. https://www.washingtonpost.com/politics/2019/12/03/russia-wants-more-influence-africa-its-using-disinformation-get-there/

[61] Alekseev, Y. "Well, Hello, "Blue Division"!" 14 June 2017. IMHOclub.lv. https://imhoclub.lv/ru/material/nu_zdravstvuj_golubaja_divizija

[62] Aleksejeva, N. "#BalticBrief: Vesti Investing in Pro-Kremlin Audience Online. Medium, 11 February 2018. https://medium.com/dfrlab/balticbrief-vesti-investing-in-pro-kremlin-audience-online-8198de3c7049#:~:text=Vesti.lv

[63] Staff Writer. "NATO Soldiers Complained of Disgusting Behaviour in Adazi." Sputnik News, 28 September 2017a. https://lv.sputniknews.ru/Latvia/20170928/5999101/Latvii-pozhalovalis-soldat-NATO-zamusorivshih-les-Adazhi.html

[64] Staff Writer. "Residents of Adazi: NATO Pigs Protect Us!" Focus, 28 September 2017b. http://ru.focus.lv/news/zhiteli-adazhi-nas-zashishayut-natovskie-svinji?18091

[65] Staff Writer. "NATO Soldiers in Latvia Pollute Forests with Household Waste." Regnum, 28 September 2017c. https://regnum.ru/news/accidents/2328026.html

[66] Staff Writer. "Social Network: NATO Soldiers Litter Adazi Like Pigs." Press, 28 September 2017d. https://press.lv/post/sotsset-soldaty-nato-musoryat-kak-svini

[67] Burma, N. https://www.facebook.com/profile.php?id=100003389608913 Facebook, 26 September 2017. Accessed: March 15, 2021, from https://www.facebook.com/photo.php?fbid=1378436735612633&set=gm.2061623364071889&type=3&theater

[68] Buholcs, J., Denisa-Liepniece, S., and Sile, E. " 'NATO – Pigs' or a Story about a Photo." Delphi, 15 November 2017. https://www.delfi.lv/news/national/politics/nato-cukas-jeb-stasts-par-kadu-fotografiju.d?id=49445411

[69] Staff Writer. "Canadian Soldiers Created Demand for Apartments in Riga." Gorod News, 11 August 2017e. https://gorod.lv/novosti/284494-kanadskie-soldaty-sozdali-spros-na-kvartiry-v-rige

[70] Kopylova, E. " 'Housing Issue' of the Canadian Military has Affected the Rental Housing Market in Riga. LSM, 11 August 2017. https://rus.lsm.lv/statja/novosti/ekonomika/kvartirniy-vopros-kanadskih-voennih-povlijal-na-rinok-arendi-zhilja-v-rige.a246392/

[71] Skumbina, M. "Specialist: Elite Housing in Riga Rented by NATO Military." EA Daily, 13 August 2017. https://eadaily.com/ru/news/2017/08/13/specialist-elitnoe-zhile-v-rige-snimayut-voennye-nato

[72] Berger, H. "Canadian Military Hit the Riga Housing Market. Vesti, 12 August 2017. http://vesti.lv/news/kanadskie-voennye-udarili-po-rynku-zhilyya-v-rige

[73] Ledeneva, A.V. 2006. How Russia Really Works: The Informal Practices that Shaped Post-Soviet Politics and Business. Cornell University Press.

[74] Staff Writer. "Expert: Instead of Barracks for NATO Soldiers, Five Schools Could Be Built." Sputnik News, 30 August 2017f. https://lv.sputniknews.ru/radio/20170830/5722245/jekspert-vmesto-kazarm-soldat-nato-mozhno-bylo-postroit-pjat-shkol.html

[75] Staff Writer. "Latvia Continues to Invest in the Militarization of the Country." Regnum, 31 August 2017g. https://regnum.ru/news/2315937.html

[76] Staff Writer. "Several Troops Had to be Sent into Isolation." Baltijas Balss, 20 April 2020a. https://bb.lv/statja/covid-19/2020/04/20/neskolko-voennoslujaschih-nato-prishlos-otpravit-v-izolyaciyu

[77] Jakubauskas, R. "There Are Eight People with Coronavirus in the Army and about 200 Soldiers in Isolation." BNS, 17 April 2020. https://www.bns.lt/topic/1912/news/61092239/

[78] Palladis, E. "Canadian Soldiers Test Positive in Latvia." The Duran, 22 April 2020. https://theduran.com/20-canadian-soldiers-tested-positive-in-latvia/

[79] Foster, L., Riddell, S., Mainor, D., and Roncone, G. " 'Ghostwriter' Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narrative Aligned with Russian Security Interests." Mandiant, 2020. https://www.fireeye.com/blog/threat-research/2020/07/ghostwriter-influence-campaign.html

[80] Staff Writer. "False News is Being Directed against NATO Soldiers in Latvia, Announcing the Mass Illness of COVID-19." SARGS.LV, 23 April 2020b. https://www.sargs.lv/lv/latvija/2020-04-23/pret-nato-karaviriem-latvija-vers-viltus-zinas-vestot-par-masveida-saslimsanu-ar?fbclid=IwAR154JDfxDGDaWstr-GGsy%E2%80%A6

[81] Staff Writer. "The Fake News Portal that Attacked NATO Soldiers Has Also Affected the French Presidential Election." SARGS.LV, 25 April 2020c. https://www.sargs.lv/lv/latvija/2020-04-25/nato-karaviriem-uzbrukusais-viltus-zinu-portals-ietekmejis-ari-francijas?fbclid=IwAR1Xe8lI3wW1ZvooEJVuc2ZgLp77L%E2%80%A6

[82] Staff Writer. "Artis Pabriks: Attempts to Attack Information Space with Deceptive Messages Area a Sign of Potential Adversary's Inferiority Complex." Ministry of Defence of the Republic of Latvia, 27 April 2020d. https://www.mod.gov.lv/en/news/artis-pabriks-attempts-attack-information-space-deceptive-messages-are-sign-potential

[83] Starikov, N. "From Unverified Sources: How the Canadian Special Forces in the Donbass Failed." Nikolay Starikov, 6 August 2016a. https://nstarikov.ru/iz-neproverennykh-istochnikov-kak-kana-69517

[84] Starikov, N. "How Canadian Special Forces in Donbass Failed." Politicus, 6 August 2016b. https://politikus.ru/events/81897-kak-kanadskiy-specnaz-na-donbasse-provalilsya.html

[85] Ivashov, G. "11 Special Forces of the Canadian Armed Forces Showed a "Master Class" in Donbass. Their Corpses were Sent on a Special Flight to Canada." CONT, 9 September 2016a. https://cont.ws/@georgyivashov/367767

[86] Ivashov, G. "11 Canadian Mercenaries Go Home in Bodybags after "Master Class" in Donbass." Stalker Zone, 13 September 2016b. http://www.stalkerzone.org/tag/cansofcom/

[87] DPR Defense Ministry. "Ukrainian Militants' Provocation Resulted in Death of Foreign Military – DPR Defense Ministry." DPR Ministry of Defence, 17 May 2018. https://archive2018-2020.dnronline.su/2018/05/17/provokatsiya-ukrainskih-boevikov-privela-k-gibeli-inostrannyh-voennosluzhashhih-stskk/

[88] Staff Writer. "Despite the Untrue Nature of the Report, it Quickly Spread on Russian-Language Social Media Accounts." UNIAN, 20 May 2018a. https://www.unian.info/world/10123442-canada-denies-russian-rumours-that-three-canadian-soldiers-were-killed-in-ukraine-media.html

[89] Makuch, B. "Pro-Russian News Once Claimed 11 Canadian Commandos Died in Ukraine. That Didn't Happen." VICE, 5 June 2018. https://www.vice.com/en/article/ywe5bk/pro-russian-news-once-claimed-11-canadian-commandos-died-in-ukraine-that-didnt-happen

[90] LeRoy, W. "Feds Deny Russian Rumours that 3 Canadian Soldiers Were Killed in Ukraine." CTV News, 19 May 2018. https://www.ctvnews.ca/politics/feds-deny-russian-rumours-that-3-canadian-soldiers-were-killed-in-ukraine-1.3936488

[91] Kassam, A. "Canada Names Chrystia Freeland, Leading Russia Critic, as Foreign Minister." The Guardian, 10 January 2017. https://www.theguardian.com/world/2017/jan/10/canada-chrystia-freeland-foreign-minister-russia-critic

[92] Ling, J. "Canada's Foreign Minister Warns of Russian Destabilization Efforts – and She Might Be a Target." VICE, 3 March 2017. https://www.vice.com/en/article/8xmyna/canadas-foreign-minister-warns-of-russian-destabilization-efforts-and-she-might-be-a-target

[93] Glavin, T. How Russia's Attack on Freeland Got Traction in Canada. MacLeans, 14 March 2017b. https://www.macleans.ca/politics/how-russias-attack-on-freeland-got-traction-in-canada/

[94] Shekhovtsov, A. "Is Russia's Insider Sponsored by a Russian Oligarch with Ties to the European Far Right?" The Interpreter, 2 November 2015. https://www.interpretermag.com/is-russia-insider-sponsored-by-a-russian-oligarch-with-ties-to-the-european-far-right/

[95] Staff Writer. "Antisemitism and Pro-Kremlin Propaganda." EUvsDisinfo, 10 January 2018b. https://euvsdisinfo.eu/antisemitism-and-pro-kremlin-propaganda/

[96] Helmer, J. "Scoop: Canada's New foreign Minister Lying about family's Ukrainian Nazi Past." Russia Insider, 19 January 2017a. https://russia-insider.com/en/victim-or-aggressor-chrystia-freelands-family-record-nazi-war-profiteering-and-murder-crakow-jews

[97] Helmer, J. "Chrystia Freeland's Family Record for Nazi War Profiteering, and Murder of the Cracow Jews." Strategic Culture, 27 January 2017b. https://www.strategic-culture.org/news/2017/01/27/chrystia-freeland-family-record-nazi-war-murder-cracow-jews/

[98] Glavin, T. "Terry Glavin: Enter the Freeland-Nazi Conspiracy – and Amping-Up of Russia's Mischief in Canada." The National Post, 8 March 2017a. http://news.nationalpost.com/full-comment/terry-glavin-enter-the-freeland-nazi-conspiracy-and-the-amping-up-of-russias-mischief-in-canada

[99] Staff Writer. "And You Are a Nazi, Too!" EU East StratCom Task Force, 26 January 2017h. https://us11.campaign-archive.com/?u=cd23226ada1699a77000eb60b&id=d50f54d197

[100] Ponce de Leon, E., and Andriukaitis, L. "Facebook Takes Down Assets Linked to Russian Disinformation Outlet." Medium, 24 September 2020. https://medium.com/dfrlab/facebook-takes-down-assets-linked-to-russian-disinformation-outlet-acab0164e3d4

[101] Staff Writer. "An Unfounded Foundation." EUvsDisinfo, 8 February 2019a. https://euvsdisinfo.eu/an-unfounded-foundation/

[102] Balcerac, S. "The New Foreign Minister of Canada Christia Freeland – Proud Granddaughter Collaborator!" Warszanka Gazeta, 8 February 2017. http://warszawskagazeta.pl/polityka/item/4562-nowa-minister-spraw-zagranicznych-kanady-chrystia-freeland-dumna-wnuczka-kolaboranta

[103] Tsukanova, A. "A Nazi Skeleton in the Family Closet." Consortium News, 27 February 2017. https://consortiumnews.com/2017/02/27/a-nazi-skeleton-in-the-family-closet/

[104] Media Bias/Fact Check. "Consortium News. Media Bias Fact Check." n.d. Accessed: 15 March 2021 from https://mediabiasfactcheck.com/consortium-news/

[105] Lauria, J. "Consortium News Sues Canadian TV Network for Defamation Over Report CN was Part of 'Attack' 'Directed' by Russia." Consortium News, 13 October 2020. https://consortiumnews.com/2020/10/13/consortium-news-sues-canadian-tv-network-for-defamation-over-report-cn-was-part-of-attack-directed-by-russia/

[106] Global Engagement Center. "Pillars of Russia's Disinformation and Propaganda Ecosystem." August 2020. https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia's-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

[107] Fife, R. "Freeland Warns Canadian to Beware of Russian Disinformation." The Globe and Mail, 6 March 2017. https://www.theglobeandmail.com/news/politics/freeland-warns-canadians-to-beware-of-russian-disinformation/article34227707/

[108] Russian Congress of Canada. "Appeal to Prime Minister Trudeau to Question Minister Freeland's Integrity. Russian Congress of Canada." 21 March 2017. http://russiancongresscanada.org/geopolitics-en/appeal-to-prime-minister-trudeau-to-question-minister-freelands-integrity/

[109] Pugliese, D. "Chrystia Freeland's Granddad Was Indeed a Nazi Collaborator – so Much for Russian Disinformation." Ottawa Citizen, 8 March 2017. https://ottawacitizen.com/news/national/defence-watch/chrystia-freelands-granddad-was-indeed-a-nazi-collaborator-so-much-for-russian-disinformation

[110] Brown, C. "Top Russian News Host Takes Aim at Ukrainian Canadians." CBC News, 17 January 2019. https://www.cbc.ca/news/world/top-russian-news-host-takes-aim-at-ukrainian-canadians-1.4980859

[111] Berthiaume, L. "Canada Expelling Russian Diplomats after Nerve Agent Attack in U.K." Huffington Post, 26 March 2018. https://www.huffingtonpost.ca/2018/03/26/canada-expelling-russian-diplomats-after-nerve-agent-attack-in-u-k_a_23395481/

[112] Pugliese, D. "Exclusive: Russian Diplomat Booted from Canada Has Some Advice for Trudeau – It Won't Work." National Post, 6 April 2018. https://nationalpost.com/news/politics/russian-diplomat-calls-expulsions-over-remarks-un-canadian

[113] Guly, C. "Smear Campaign Against Freeland Linked to Russian Diplomats' Expulsion, Says Trudeau." The Ukrainian Weekly, 13 April 2018. http://www.ukrweekly.com/uwwp/180711-2/

[114] Fife, R. and Carbert, M. "Russian Spies Aimed to Discredit WADA, Spread Disinformation about Canada with Cyber Campaigns. The Globe and Mail, 29 March 2018. https://www.theglobeandmail.com/politics/article-russian-spies-aimed-to-discredit-wada-spread-disinformation-about/

[115] Staff Writer. "Donbass Militia Spots Mercs from US, Canada, Baltics, Poland in East Ukraine. Sputnik News, 16 October 2016. https://sputniknews.com/europe/201610161046389363-donbass-reconaissance-foreign-mercenaries/

[116] Chase, S. "NATO Mission in Latvia Unwise Diversion from Terror Fight: Russian Envoy." The Globe and Mail, 21 December 2016. https://www.theglobeandmail.com/news/politics/nato-mission-in-latvia-unwise-diversion-from-terror-fight-russian-envoy-says/article33397586/

[117] Fisher, M. "Matthew Fisher: Sajjan a Target of Russian Cyber Campaign Aimed at Undermining NATO's Presence in Baltic Republics." National Post, 14 May 2017. https://nationalpost.com/news/world/matthew-fisher-sajjan-a-target-of-russian-cyber-campaign-aimed-at-undermining-natos-presence-in-baltic-republics

[118] Staff Writer. "NATO Soldiers in Latvia Will Be Able to Carry Loaded Weapons." Mix News, 8 March 2017i. http://www.mixnews.lv/ru/society/news/217875_soldaty-nato-v-latvii-smogut-nosit-zaryazhennoe-oruzhie/

[119] Staff Writer. "DUI GIs? NATO Troops in Estonia Crash Three Vehicles in Two Days." Sputnik News, 20 May 2017j. https://sputniknews.com/military/201705201053819143-nato-estonia-drills-mishaps/

[120] Staff Writer. "Estonian Man with Shotgun Chases Away Trespassing NATO Troops." Sputnik News, 25 May 2017k. https://sputniknews.com/europe/201705251053983605-estonian-man-chases-away-nato-troops/

[121] Staff Writer. "Drunken German NATO Members Beaten in Lithuania." Sputnik News, 4 June 2017l. https://m.lv.sputniknews.ru/Baltics/20170604/4944848/Pjanye-nemeckie-NATOvcy-pobity-v-Litve.html

[122] Wasserman, A. "Memo for Latvians: Think Twice Before Refusing a NATO Soldier." Sputnik News, 20 June 2017. https://m.lv.sputniknews.ru/columnists/20170620/5093872/anatolij-vasserman-pamjatka-latyshkam-pribytie-soldat-nato.html

[123] Staff Writer. "NATO Soldier Relieved Himself on the Building of the Ministry of Interior of Lithuania." Sputnik News, 22 June 2017m. https://m.lv.sputniknews.ru/Baltics/20210421/15546201/Premer-Estonii-zayavila-chto-strane-pograndogovor-nuzhen-bolshe-chem-Rossii.html

[124] Staff Writer. "NATO Maneuvers Caused Anxiety Among the Residents of Lithuania." Sputnik News, 1 July 2017n. https://m.lv.sputniknews.ru/Baltics/20170701/5209992/natovskie-manevry-vyzyvajut-bespokojstvo-zhiteli-litva.html

[125] Staff Writer. "To Pay or Not to Pay: NATO Military Staged a Fight in a Restaurant in Vilnius." Sputnik News, 2 July 2017o. https://m.lv.sputniknews.ru/Baltics/20170702/5214761/platit-ili-ne-platit-voennye-nato-ustroili-draku-restoran-vilnjus.html

[126] Lompar, G. "US Military Bio-Labs in Ukraine, Production of Bio-Weapons and 'Disease Causing Agents.' " Global Research, 24 August 2017. https://www.globalresearch.ca/us-military-bio-labs-in-ukraine-production-of-bio-weapons-and-disease-causing-agents/5605307

[127] Staff Writer. NATO Soldiers Humiliate the Population of the Baltics. Gorod News, 18 October 2017. https://gorod.lv/novosti/286828-soldaty-nato-unizhaut-naselenie-baltii

[128] Shinkman, P.D. Russia Hacked Latvia's Cellphone Network During Massive Military Exercise. US News, 24 November 2017. https://www.usnews.com/news/world/articles/2017-11-24/russia-hacked-latvias-cellphone-network-during-massive-military-exercises

[129] Trevithick, J. "Russia Jammed Phones and GPS in Northern Europe During Massive Military Drills." The Drive, 16 October 2017b. https://www.thedrive.com/the-war-zone/15194/russia-jammed-phones-and-gps-in-northern-europe-during-massive-military-drills

[130] Dapkus, L. 2018, January 19. Lithuania Probing Bogus Story after TV Station is Hacked. AP. https://apnews.com/article/a572abd0c8d44da3bfe6609746510247

[131] Bankauskaite, D., and Celutka, S. "Cyberattacks in Lithuania: The New Normal." StopFake.Org., 6 May 2018. https://www.stopfake.org/en/cyberattacks-in-lithuania-the-new-normal/?__cf_chl_jschl_tk__=2234fc40e6a8f5fba766cccf8e84bd8e51dda9eb-1579488067-0-ATdQwP4DiHbXoPbbeqWDK ta2dsrqq93ISVZMB3hPR0Bo6TyZ4UB52s59NqE3I6Oygpl7XGheB7Y96f8Vw2EfDbtR_Kfk5dDw sgebazqanwzcP44BFsN5otgcAdyxsUS0jS-LA9dLEEyL1InJVXX8GqLoZ_dGcLNGrx62-2MYwptg CQv54gwz9Vv0dmAtig0YFhHTuqPpMpAqXHtuS4kuGdJQMYiNnzNx5z-MxieLDGcKwo_tnay7f6FSsdOX0ygRP2b3sSSA-s4hABOa6Be49BK8broOeclWms_IvR11YzrQHRpqzk4B-g1rWsVZ0nxQJQ

[132] Staff Writer. "Fake News: A Child Did Not Die During NATO Military Exercise in Lithuania! The Baltic Course, 8 June 2018c. http://www.baltic-course.com/eng/modern_eu/?doc=140643

[133] EUvsDisinfo. "Disinfo: A Child Died During NATO Military Exercises in Lithuania." EUvsDisinfo, 8 June 2018. https://euvsdisinfo.eu/report/a-child-died-during-nato-military-exercises-in-lithuania/

[134] Staff Writer. "Kiev Issues Ukrainian Passports to the American Military to Enter Russia." Novorossiya News, 5 March 2019b. https://novorosinform.org/762656

[135] Aleksejeva, N. "Lingering Infektion: Latvian Operation Mimicked Secondary Infektion Tactics." Medium, 10 December 2019. https://medium.com/dfrlab/lingering-infektion-latvian-operation-mimicked-secondary-infektion-tactics-bc0bb62eacaa

[136] Beniusis, V. "Fake News Target NATO Exercises; Several News Websites Hacked in Latvia and Lithuania." LRT News, 20 June 2019. https://www.lrt.lt/en/news-in-english/19/1071172/fake-news-target-nato-exercises-several-news-websites-hacked-in-latvia-and-lithuania

[137] Sabbagh, D. "Russia-Aligned Hackers Running Anti-NATO Fake News Campaign – Report." The Guardian, 30 July 2020. https://www.theguardian.com/technology/2020/jul/30/russia-aligned-hackers-running-anti-nato-fake-news-campaign-report-poland-lithuania

[138] Tucker, P. "Russian Trolls Are Hammering Away at NATO's Presence in Lithuania." Defense One, 3 December 2019. https://www.defenseone.com/technology/2019/12/russian-trolls-are-hammering-away-natos-presence-lithuania/161654/

[139] Vandiver, J. "Lithuania Says Statement about Accepting US Nuclear Weapons is Fake." Stars and Stripes, 18 October 2019. https://www.stripes.com/news/lithuania-says-statement-about-accepting-us-nuclear-weapons-is-fake-1.603616

[140] Tlis, F. "US Army Sergeants Arrested for Carjacking BMW in Lithuania?" Polygraph., 23 December 2019. https://www.polygraph.info/a/fact-check-us-army-lithuania-cyber-attack/30341011.html

[141] Romanenko, N. "Donbass Today: The Names of Canadian Intelligence Officers in Ukraine Are Revealed, a Child is Wounded in DPR." RIA FAN, 23 March 2020. https://riafan.ru/1261448-donbass-segodnya-raskryty-imena-kanadskikh-razvedchikov-na-ukraine-v-dnr-ranen-rebenok

[142] Trevithick, J. "Russia Breaks into US Soldiers' iPhones in Apparent Hybrid Warfare Attacks." The Drive, 4 October 2017a. https://www.thedrive.com/the-war-zone/14867/russia-breaks-into-us-soldiers-iphones-in-apparent-hybrid-warfare-attacks

[143] Grove, T., Barnes, J.E., and Hinshaw, D. "Russia Targets NATO Soldier Smartphones, Western Officials Say." Wall Street Journal, 4 October 2017. https://www.wsj.com/articles/russia-targets-soldier-smartphones-western-officials-say-1507109402

[144] Fingas, J. "Russia is Hacking the Phones of NATO Soldiers." Engadget, 5 October 2017 https://www.engadget.com/2017-10-05-russia-hacks-nato-soldier-phones.html

[145] Bellingcat. "Guccifer Rising? Months-Long Phishing Campaign on ProtonMail Targets Dozens of Russia-Focused Journalists and NGOs." Bellingcat, 10 August 2019. https://www.bellingcat.com/news/uk-and-europe/2019/08/10/guccifer-rising-months-long-phishing-campaign-on-protonmail-targets-dozens-of-russia-focused-journalists-and-ngos/

[146] Asokan, A. " 'Fancy Bear' Hacking Group Adds New Capabilities, Targets. Bank Info Security." 26 September 2019. https://www.bankinfosecurity.com/fancy-bear-hacking-group-adds-new-capabilities-targets-a-13150

[147] Area 1 Security. Phishing Burisma Holdings. 2020. https://cdn.area1security.com/reports/Area-1-Security-PhishingBurismaHoldings.pdf

[148] Sharma, A. "Russian Hackers Use Fake NATO Training Docs to Breach Govt Networks." Bleeping Computer, September 2020. https://www.bleepingcomputer.com/news/security/russian-hackers-use-fake-nato-training-docs-to-breach-govt-networks/?fbclid=IwAR3u7p7z_5ONxz_IujKDZhsSrZ-C0sApD2FUh_63hv5wRrO0eKv2mdvIywk

[149] Frenkel, S. "How a Fake Group on Facebook Created Real Protests." The New York Times, 14 August 2018. https://www.nytimes.com/2018/08/14/technology/facebook-disinformation-black-elevation.html

[150] Hybrid Centre of Excellence. "Trends in the Contemporary Information Environment: Hybrid COE Expert Pool Meeting on Information (Trend Report 4)." May 2020. https://www.hybridcoe.fi/wp-content/uploads/2020/05/Hybrid-CoE-Trend-Report-4.pdf

Chapter 6 – CONCLUSION

The case studies in this volume demonstrate the importance of close study of Russian, or any threat actor's, behaviors, in a manner cognizant of the specific context of that actor. In other words, seeking to identify generic threat characteristics is less useful for planning purposes than understanding each threat on its own, at least in the first instance. The examination of KFOR and Canadian deployments to Latvia and Ukraine expose some erroneous assumptions of likely Russian behavior and targets. This conclusion is shared by several of the case studies presented in Volume III of the SAS-161 reporting. Jarl's and Lauder's case studies suggest some divergent conclusions. Whereas Jarl's case study illustrated centralization of control and interconnected, complementary military, political, and informational dimensions for Russian strategic level messaging related to large military exercises, Lauder's case study exposes decentralized execution and more simplistic means of execution. The characteristics noted by Lauder can be seen in the description of Russian activity in other case studies as well, notably Reader's and Bērziņš' chapters in Volume III. Much like the Finnish case study presented in Volume IV of our reporting, the Ukrainian case study here illustrates the high value of evidence and expertise required for the development of plausible scenarios. For both near- and long-term military planning, a net assessment approach demands that any scenarios developed are grounded in as much evidence as possible to ensure plausibility. This is the case even when the intent is to push the bounds into low likelihood, high impact types of events. This rule holds true regardless of the scenario purpose – exercise or experimentation, forecasting, foresight, or near-term planning. Finally, the scenario development described in the case study employs updated Ukrainian legal, policy, and doctrinal frameworks to set the context of the development process and analysis of the scenarios. This contributes to the proven high accuracy reflected in later real-world events. This example thereby reinforces the importance of comprehensive national level security and defence arrangements – a conclusion mirrored in the case studies in Volumes III and IV of our reporting.

Annex A – TABLE OF IMPLICATIONS-SOURCE MATERIAL

This table indicates the relationship between the various components of RTG research and analysis and the individual military implications detailed in Volume V.

Military Implication Title	Source Material
Developing Common Understanding	CAN, DNK (KFOR), GBR
Systematic Analysis of Military Exercises	GBR, SWE
Spirituality and Religion	DNK (KFOR)
Religious Organisations and Politics	DNK (KFOR)
National Interests, Alliances, and Partners	UKR
Reducing Coercive Options: Limiting Dependence	UKR
Formulating Legal Frameworks	CZE, HRV, UKR, NSHQ
NATO Capability and Capacity Building	NSHQ
NATO-UN Partnerships	DNK (KFOR)
Article 5, Hybrid Methods, and Alliance Cohesion	GBR, NSHQ
Indications, Warnings, and Article 4	GBR
Finding Common Ground	DNK (KFOR)
Adapting Force Structure	UKR, NSHQ
Situational Picture and Awareness	CZE, FIN, HRV, UKR
Wartime Military Effectiveness	UKR
NATO Operational Planning: Long-Term Threat	All material
Laws of War	UKR, NSHQ
Integration of Military and Non-Military Capabilities	UKR, NSHQ
Ukraine's Information Security: Mental Resilience	UKR
Strategic Communications and Internal Resilience	UKR
CIMIC in a National/Allied Context	DNK (KFOR)
Exercise Analysis: Frontstage (Public), Backstage (Veiled) and Mystification	CAN, SWE
Military Strategies to Handle Russian Backstage and Frontstage Acting	SWE
The Application of the Military Instrument of Power (MIOP)	GBR
MIOP Backstopping Hybrid Activity	GBR, SWE, UKR
Electronic Warfare: Prevention and Protection	FIN, HRV, SWE
Homeland Defence is the Bedrock of Alliance Cohesion	CZE, FIN, HRV, UKR
National Homeland Defence Concepts	CZE, FIN, GBR, HRV, NSHQ

Military Implication Title	Source Material
Business and Investment – The Economic Instrument of Power	FIN, HRV
Influence on Non-Governmental Organizations	DNK (KFOR), FIN, HRV
Homeland Defence: Readiness	All material
Strategic Communication in Transition: 'Total War' to 'Post-(Major) Conflict'	UKR
NATO Strategic Communications and Shared Understandings	All material
Countering Russian Rhetoric	All material
Focus on the Effect	CAN, GBR, UKR
Minor Actions Matter	CAN, GBR, UKR
Operational Security	CAN, FIN, GBR, UKR

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-SAS-161-VOL-II AC/323(SAS-161)TP/1173	ISBN 978-92-837-2485-8	PUBLIC RELEASE

5. Originator

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

The NATO STO SAS-161 Research Task Group (RTG) – Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices
Volume II: Information and Influence

7. Presented at/Sponsored by

This volume of SAS-161 presents case studies from Canada, Denmark (focused on Kosovo), Sweden, and Ukraine. All investigate various aspects of Russian information and influence activities.

8. Author(s)/Editor(s)	9. Date
Multiple	February 2024
10. Author's/Editor's Address	**11. Pages**
Multiple	124

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Backstage; Exercise; Frontstage; Hybrid; Influence operations; Information activities; Information confrontation; Information operations; KFOR; Kosovo; Latvia; Russia; Scenarios; Trident Juncture; Zapad

14. Abstract

The NATO STO SAS-161 Research Task Group (RTG) investigating "Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices" is meant to inform the full spectrum of military planning at the Alliance and national level. The functionally oriented analysis and the country-specific case studies developed by the RTG touch all aspects of military effectiveness and help inform our collective efforts to account for the challenges of contemporary, and expected future characteristics, of competition, conflict, warfare, and warfighting. This volume presents case studies that investigate various aspects of Russian information and influence activities.

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

DIFFUSION DES PUBLICATIONS

STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

BULGARIE
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DGSIST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Acquisition and Logistics Organization
(DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESPAGNE
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM), C/ Arturo Soria 289
28033 Madrid

ESTONIE
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

ETATS-UNIS
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FINLAND
Ministry for Foreign Affairs
Telecommunications Centre (24/7)
P.O BOX 176
FI-00023 Government

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25, H-1885 Budapest

ITALIE
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research
Establishment
Attn: Biblioteket

PAYS-BAS
Royal Netherlands Military
Academy Library
P.O. Box 90.002, 4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROUMANIE
Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIE
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

TCHEQUIE
Vojenský technický ústav s.p.
CZ Distribution Information
Mladoboleslavská 944
PO Box 18, 197 06 Praha 9

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Brussels

BULGARIA
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2, 1592 Sofia

CANADA
DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

CZECHIA
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18, 197 06 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5, 2750 Ballerup

ESTONIA
Estonian National Defence College
Centre for Applied Research
Riia str 12, Tartu 51013

FINLAND
Ministry for Foreign Affairs
Telecommunications Centre (24/7)
P.O Box 176, FI-00023 Government

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALY
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street, Sector 6
061353 Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen. M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SPAIN
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

TÜRKIYE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down, Salisbury SP4 0JQ

UNITED STATES
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2, CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example, AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).

ISBN 978-92-837-2485-8