THREAT-DEFUSER: Mitigating Perceived Threats in Russian and Norwegian Public Discourse
THREAT-DEFUSER integrates state-of-the-art political science, linguistics, and media studies methods to forge a new multidisciplinary approach to hybrid warfare. The primary objective is long term strategic competence on hybrid warfare in Norwegian and Russian media that empowers citizenry, policy makers, and academics to recognize and mitigate the escalation of radicalization. The project will generate high quality research findings on technologically disseminated disinformation and its role in geopolitics and, thus, foster societies resilient to hybrid warfare. The secondary objectives are to a) address a knowledge gap for three languages (North Saami, Norwegian, Russian) with quantitative linguistic analyses and qualitative methods assessing media practices to triangulate data and produce new knowledge; and b) strengthen the Norwegian research community by building a network dedicated to hybrid warfare analysis stratified to include both early-career (postdoc) and senior scholars.

1. Excellence

1.1 State of the art, knowledge needs and project objectives

Threats today – characterized as hybrid threats – increasingly emerge from diverse, non-violent methods designed to amplify fragmentation and create chaos in a target state (Singer & Brooking 2018). THREAT-DEFUSER reduces the vulnerabilities exposed by existing socio-political cleavages through state-of-the-art detection and analysis of the quality of threats and their means of dissemination, and enhances civilian resilience with a NewsRadar tool for navigating biases in news media. The example of Anders Behring Breivik highlights the dangers of ideologically extreme Internet "tribes". THREAT-DEFUSER uses sophisticated quantitative and qualitative methods to identify unreliable news sources that galvanize polarising ideologies and to alert the public to promote understanding instead of potential radicalization.

THREAT-DEFUSER draws on Norway's strengths in finding peace-oriented solutions to security threats. THREAT-DEFUSER increases Norwegian capacity to address challenges of disinformation in relation to Norway's biggest neighbor: Russia. Today's geopolitical situation is characterized by precarious relations between Russia and a number of NATO states. Norway is obligated both by the politics and narratives emanating from its NATO membership, and by its complex, successful (economic, social, cultural) relationships across the Norwegian-Russian border. THREAT-DEFUSER has a crucial role to play in mitigating misunderstandings and radical positions produced by disinformation in hybrid warfare scenarios.

Academic disciplines tend to be disproportionately focused on the English-speaking world. THREAT-DEFUSER breaks away from that narrow view, focusing instead on Russian and two official languages of Norway: Norwegian and North Saami. Three cultural perspectives are opened up: 1) a major international language, since Russian is among the most-used languages on the Internet; 2) a majority national language; 3) a minority indigenous language. The tools created by THREAT-DEFUSER are portable to other languages, cultures, and domains, and will be shared open source with the international research community.

For external (foreign) actors it is more effective to destabilize a state by making use of existing conflict cleavages. With the developments in cyber/digital technologies and diverse media platforms, this is becoming easier than ever. THREAT-DEFUSER targets precisely the ways in which these cleavages are polarized and exacerbated through digital technologies. THREAT-DEFUSER delivers analyses and products with the aim of strengthening the resilience of civilians subjected to these radicalizing interventions.

Targeting vulnerabilities is a central part of hybrid warfare today. Destabilization can arise in the face of existing vulnerabilities within a state's society or amongst its citizens, and is easily propagated through media. Hybrid disinformation targets existing citizen threat perceptions which are influenced, generated, and manipulated through media. Perceptions of threats are inherently linked to perceptions of insecurity. The spread of misleading and/or false information can exacerbate unrest due to economic difficulties such as job loss, migration, and consequences of climate change. Destabilizing effects occur when citizens have reduced trust in political structures and institutions to address their security needs, and/or have reduced trust between each other, making societies and states vulnerable to escalation of conflict.

Determining sources of destabilization can be difficult, particularly when media is used to disseminate disinformation. Purposeful attacks or attempts to create distrust and instability are difficult to attribute directly to specific actors (Reichborn-Kjennerud & Cullen 2016) since they often result from a combination of internal and external actors, whereby internal vulnerabilities become manipulated by external actors.

In response, various international organizations and states are focusing on resilience in society as an antidote to hybrid disinformation that targets threat perceptions. Resilience can be defined as "the ability of an individual, a household, a community, a country or region to withstand, cope, adapt, and quickly recover from stresses and shocks such as violence, conflict, drought and other natural disasters without compromising long-term development" (EuropeAid 2016, and for critique see Chandler & Reid 2016). The concept has increased its relevance to internal and "near neighbour" contexts whereby resilience becomes "the ability to absorb, adapt and recover from shocks through a number of initiatives within the EU itself, as well as through resilience-building measures in regions adjacent to the EU – namely through democracy, human rights, and the rule of law" (Sørensen & Nyemann, 2018: 2). Citizen actions and reactions to crisis have a clear impact on destabilization (Fearon 1994). Though resilience of citizens and communities is crucial, little in the way of concrete measures have been taken to enhance resilience at the citizen level. Conflict historian Margaret MacMillan emphasized in her 2018 Reith lecture series that deconfliction is dependent upon understanding "the other", particularly from the grassroots level. THREAT-DEFUSER does just that, focusing on how information and disinformation are propagated and used to influence/manipulate citizens in different communities for the purpose of destabilizing those same communities.

Citizen actors engage in diverse strategies to ensure human security (primarily physical and economic), including cooperation with armed groups (state or non-state), selective sharing of information and resources, the spread of dis/misinformation, and everyday forms of resistance (Jose and Medie 2015, Hoogensen Gjørv under review). Citizen agency is often framed as "resilience" but can include resistance (to other citizens, governments, institutions), and includes multiple subjects of resilience that can be contradictory (Cavelty, Kaufmann et al. 2015). It includes all activities approaching (but not including) the use of violence if conflict drivers among citizens are excessively aggravated (Heffington 2017).

THREAT-DEFUSER examines language that directly targets perceived vulnerabilities, e.g. terrorism, nationalism, populism, migration, climate change etc. The societal challenges are complex, calling for an integrated interdisciplinary approach. We combine linguistic analysis of the big data of language corpora and path-breaking techniques developed in the Czech Republic with social science approaches such as document, discourse, and intersectional analyses of how language is gendered, racialized, and classed to trigger emotional reactions in populations and exacerbate conflict cleavages in societies. THREAT-DEFUSER integrates these methods to develop tools of analysis for Russian, North Saami, and Norwegian media.

Messages convey more than content. Their language has the potential to reveal sources and biases. Already in 1963, Mosteller and Wallace challenged a 175-year-old mystery concerning the authorship of twelve of the Federalist Papers. Blatt (2017) fingerprints individual writers by looking at the relative frequencies of common words and other features of their texts. Keyword/Keymorph Analysis (Baker 2004, 2006; Baker & McEnery 2005; Scott & Tribble 2006) enables us to go beyond mere identification of sources to disclose their (often hidden) agendas. Keyword/Keymorph Analysis works by creating a yardstick to detect and measure differences from the norm in a language. The yardstick is a "reference corpus", a large sample (on the order of millions or billions of words) that represents a model speaker of that language. A reference corpus makes it possible to detect ideological bias in media that otherwise "creates the impression of objective and well-balanced news" by discovering "language patterns that are prominent against the background of general language usage" (Fidler & Cvrček 2018: 195,221). Bias can be delivered in the guise of seemingly innocent ordinary words, such as prepositions, adverbs and geographical terms (Keywords), as well as grammatical categories, such as case (marked by Keymorphs), and collocations. The Keywords and Keymorphs emerge as statistical outliers (deviant items) when a target sample is compared against the reference corpus using Keyword/Keymorph Analysis. In other words, Keyword/Keymorph analysis makes it possible to discover how specific texts differ from the backdrop of ordinary use in a language by identifying words and forms that appear much more frequently than one would expect. Researchers do not a priori select words or forms that they suspect to be ideologically "loaded", an approach that would be narrower in scope and ultimately circular in the logic of its application. Instead, the entirety of relevant Keywords and Keymorphs emerge from the comparison and are then analyzed a posteriori. This quantitative process facilitates the identification of specific texts that deserve a "deep dive" via intensive qualitative analysis (for examples of the latter, see Krüger 2016 and MacLeod 2019). Fidler & Cvrček (2018) analyzed texts focusing on the conflict in Ukraine produced by *Sputnik Česká Republika*, a Czech-language news site based in Moscow, concluding that this Kremlin-sponsored news venue is pushing a pro-Russian agenda. What is remarkable is that this agenda is conveyed by seemingly "neutral" words, and that the covert ideological slant can be revealed by comparing target texts to a reference corpus. For example, among Fidler & Cvrček's many striking findings was differential use of case morphology: Putin appeared disproportionately often in the Nominative and Instrumental cases, emphasizing his role as an agent and collaborator, whereas Ukraine's leader Poroshenko was associated with the Dative case, casting him as a passive experiencer. Fidler & Cvrček (2018) present a proof-of-concept suggesting that Keyword/Keymorph Analysis can detect any type of bias, not just bias that we already suspect to be present. THREAT-DEFUSER takes Keyword/Keymorph Analysis in several new directions, expanding it to new languages and media sources.

Target samples for our analysis focus on the language of threats as conveyed in Norwegian, North Saami, and Russian. Here we see that cultures differ in how perceptions of threats are encoded in their languages. THREAT-DEFUSER develops vocabularies to facilitate extraction of target samples starting from words such as 'security', 'hybrid warfare', 'military', 'immigration', 'threat', 'climate change', 'terrorism' and analyzing their collocates and embeddings (words that co-occur, indicating associated meanings and synonyms). Statistical analysis of collocates reveals the rich and often language-specific patterns of word meanings, since we "know a word by the company it keeps" (Firth 1957: 11). Adjectives next to a noun like 'threat' further specify the meaning of that word. We see such patterns in the Aranea Family of Gigaword Web Corpora (Benko 2014), where the five most frequent adjectives next to Norwegian *trussel* 'threat' are *stor* 'big', *alvorlig* 'serious', *reell* 'real', *direkte* 'direct', and *potensiell* 'potential'. The first four adjectives next to Russian *ugroza* 'threat' are similar: *real'naja* 'real', *ser'eznaja* 'serious', *potencial'naja* 'potential', *prjamaja* 'direct'. But in fifth place is the Russian phrase *vnešnjaja ugroza* 'external threat' at a rate of 0.43 per million words, and not far behind it *vnutrennjaja ugroza* 'internal threat' at 0.24 per million words. By contrast, Norwegian equivalents for 'external/internal threat' appear at only 0.01 per million words. In other words, Russian shows a persistent focus on external/internal threats that is lacking in Norwegian discourse. Collocates of indigenous North Sami *áitta* 'threat' highlight concerns about climate change and implications for fish, reindeer, and nature, revealing that North Saami, even though it shares the same region, differs in its framing of threats as opposed to Norwegian and Russian. Word embeddings (not available for North Saami) uncover synonyms by revealing what words keep company with the same collocates. Figure 1 juxtaposes visualizations of word embeddings for Russian and Norwegian words for 'terrorism'. Both languages highlight extremism and organized crime, but while Russian brings out corruption and separatism, Norwegian focuses on Islam and the far right.

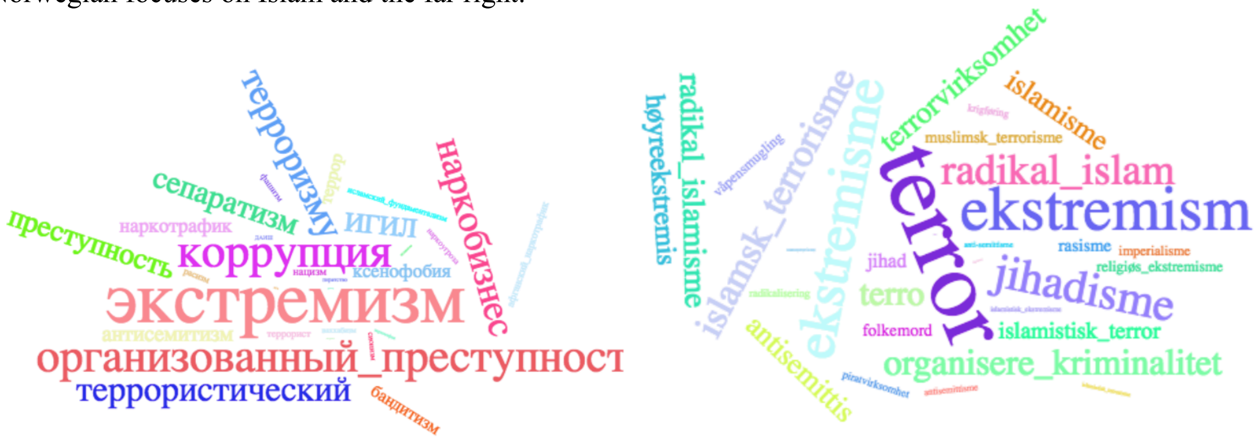

Figure 1: Word cloud visualizations of word embeddings (synonyms) for 'terrorism' in Russian and Norwegian

In addition to mapping out cultural and linguistic differences, it is necessary to detect patterns in how messages are propagated. Šlerka and Šisler (2017, 2018) have pioneered methods for mapping out the interconnectivity between news media sources by tracking the Facebook "likes" of posts measured in terms of Normalized Social Distance. This makes it possible to classify media sources on a multidimensional scale ranging from neutral to strongly deviant in an open-ended number of directions, including everything from mainstream investigative reporting to far right/left and other extremist sources that divide public discourse, and are exacerbated by social media and browser algorithms to create "tribes" that are intellectually and morally isolated from each other. THREAT-DEFUSER develops this method for a multimodal project that analyzes threat-related target samples from Internet/Newspaper, TV (via closed caption text), and podcasts (via transcripts) across the full spectrum of the Norwegian, North Saami, and Russian media market.

1.2 Novelty and Ambition

THREAT-DEFUSER is innovative and ambitious on three levels:

- Data collection – collecting and combining social science and linguistic data (both quantitative and qualitative) pertaining to a leading security concern;
- Data analysis – combining various analytical tools (linguistic and intersectional);
- Prototype development – creating the NewsRadar browser plug-in/extension to be used by citizens and policy makers to analyze and reduce vulnerability to disinformation, promoting citizen science.

THREAT-DEFUSER forges a new amalgam of the foremost strengths of automated political, linguistic, and media analysis. We make no a priori assumptions or categories, instead facilitating the emergence of new knowledge directly from the data of language use and social media connectivity. Using reference corpora as a lens, through Keyword/Keymorph analyses we reveal the biases across the spectrum of news media sources that are at once highly influential and "hidden in plain sight". In addition to scholarly articles, policy recommendations, and an open-access website, THREAT-DEFUSER will put a concrete product in the hands of the public: the NewsRadar plug-in app that alerts media consumers to issues concerning connectivity (or lack thereof) and biases of news sources.

1.3 Research questions and hypotheses, theoretical approach and methodology

The central hypothesis of THREAT-DEFUSER is that we can help citizens to be resilient in the face of hybrid warfare. Systematic delivery of media ratings and alternatives can help bridge societal divides. This hypothesis is elaborated by corollary research questions (RQs):

RQ1: How does the language of threats differ across Russian, Norwegian, and North Saami?
RQ2: How does the profile of threat portrayal differ across media sources in Russia and Norway?
RQ3: Which media sources in Russia and Norway are more connected vs. isolated in relation to others?
RQ4: To what degree are average citizens targets for the manipulation of threat language and to what ends?
RQ5: What tools can assist citizens in identifying bias and obtaining balanced media messages?

Differences in threat portrayal and media connectivity are related to each other: media sources that portray threats similarly tend to have overlapping audiences, but may be isolated from media sources that differ in threat portrayal. Analysis of threat portrayal and connectivity can establish a map of the relative position of media sources. By providing ratings of media sources we can nudge society toward unity and understanding of the "other" and mitigate the dangers of radicalization. THREAT-DEFUSER focuses specifically on how samples of threat discourse differ from a reference corpus and how media connectivity promotes and/or hinders propagation. Evaluation of the veracity of threat portrayals (as legitimate vs. "fake news") is, however, not within the scope of the project.

Theoretical approach: THREAT-DEFUSER combines social science and linguistic theories and methods. It delivers linguistic analysis within the frameworks of cognitive linguistics (Janda 2015) and corpus linguistics, and more specifically follows the lead of Keyword/Keymorph Analysis as established by Fidler & Cvrček (2018). The measurement of media connectivity in terms of Normalized Social Distance has been pioneered by Šlerka & Šisler (2017, 2018) and is grounded in a quantitative branch of new media studies. Figure 2 displays an example, mapping the Normalized Social Distance of Czech media sources, with mainstream sources in violet in the lower right, right-wing sources in orange in the upper left, and tabloid sources in green on the lower left.

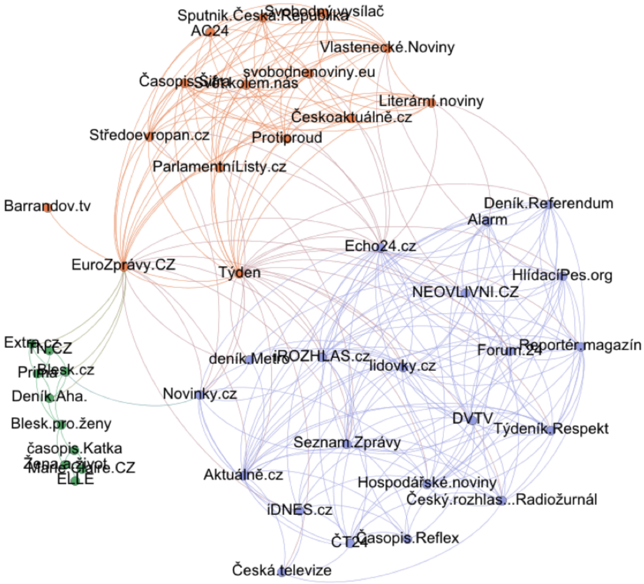

Figure 2: Czech media connectivity

In addition, THREAT-DEFUSER will focus on the interplay between institutional and individual forms of trust, providing empirically grounded insights into the role of emotions (especially fear and anger) in populism and extremism, and the role of media technologies and institutions in these processes. Intersectional analyses (rooted in critical feminist security studies) will be employed to understand processes of populism and extremism in Norway, examining how individuals and groups receive and respond to the communication of threats and to what degree such threats foster populism and extremism. We will collect and examine open access/public sites on different media that promote or disseminate information that can be used to increase fear and anger or promote potentially conflictual activities (rallies, hate speech, vandalism, incitement to physical violence).

Method: THREAT-DEFUSER develops language-specific threat vocabularies for Russian, Norwegian, and North Saami based on the behavior of collocates and word embeddings in reference corpora. These vocabularies reflect the culture-specific profiles of threat discourse, showing unique statistical distributions and linguistic behaviors in conceptual representation of threat across the three languages. The threat vocabularies facilitate extraction of target texts containing threat-related discourse from a range of media sources. Computational tools can be trained on a small number of selected texts to detect a larger sample of target texts containing threat discourse (Baisa et al. 2017). Target texts are submitted to Keyword/Keymorph Analysis, revealing ideological patterns in measurable ways by means of comparison with reference corpora. One way of measuring the connectivity of media sources is by tracking likes of Facebook posts and applying the mathematical formula for Normalized Social Distance (based on the numbers of members in audiences, their intersection, and the total number of members overall). Results from analysis of media connectivity and ideological patterns can be merged to yield ratings of media sources. The NewsRadar app reports these ratings as advisories when consumers access news feeds.

A remarkable finding in the Czech media connectivity visualized in Figure 2 is that the tabloid sources that are isolated as a group (those in green) are largely media that target women (with titles such as *ELLE*, *Marie Claire.cz* and *Žena a život* ‘Woman and life’). Many news services are predicated upon appeal to audiences defined by gender identity. THREAT-DEFUSER will determine how such gendered media behave in Norwegian and Russian public discourse.

Intersectionality tells us that gender, race, ethnicity, class, etc. are central social and political dimensions of human societies. Intersectional research is part of the broader domain of social sciences, which itself has experienced “science wars”, a contestation of methodologies, methods, and approaches (Keating & Della Porta 2010). Social sciences operate at high levels of abstraction, where social inquiry includes exploring ontologies, epistemologies, methodologies, and methods without predetermining the process of inquiry. As such, different processes of inquiry result in different constructions and productions of knowledge. In other words, social science methods, including discourse analysis, question assumptions in allegedly objective methods in an attempt to identify and balance out potential hidden biases. Intersectional approaches, which have been developed particularly within certain segments of feminist scholarship, analyze the ways in which the positionality and subjectivity of both the researcher and the citizen influence understandings of threats.

Feminists have long called attention to a gendered and masculinist bias within concepts and approaches to scholarship, not least exemplified by the emphasis on rationality, objectivity, and public domains, often embodied by research in the natural sciences and reinforcing “an unreflective orientation toward objectivist traditions and norms” (Gray 2017: 180). A core feature of feminist and intersectional methodological approaches therefore includes the practice of “reflexivity” whereby the researcher is “‘responsible’ and ‘responsive’ to her work and her ‘subjects’ of study because it makes explicit the deliberative movement of her scholarship” (Ackerly et al. 2006). Reflexivity allows for insight into phenomena while also illuminating how such insights were derived: “the closer an academic discipline is aligned with the natural science model the greater the pressure can be to engage in un-reflexive silent authorship” (ibid). Thus, the dominance of a natural science-heavy scholarship informed by objectivist methods plays a significant role in the acceptance and comprehension of what intersectional analyses bring to the discussion. Our intention is not to discredit objectivist/positivist types of study, as these bring necessary knowledge to light. This research instead expands its analytical scope to benefit from a more substantial engagement with diverse methods and voices and provide complex insights into the broader social and political contexts in which this research takes place.

An intersectional analytical approach has the ability to transcend and integrate many of the levels and sectors of security that scholars have otherwise chosen to analyze separately. Instead of playing into the dominant approaches to security studies which focus on a very small portion of the security grid from the top down, gender analysis takes its starting point from the bottom up; it reaches all the way down to the individual, as gender analysis acknowledges that even the personal is political, and therefore the individual's experience is relevant. At the same time it is recognized that individuals are part of communities, and that gender is a significant feature of individual identity in relation to others and is therefore a part of societal security (Hoogensen and Rottem 2004). The social constructions of gender come into play in the analysis, and the ways in which humans have constructed their societies on the basis of gender roles, who has the "right" to play which roles in the society, and how people are supposed to relate to one another. Intersectional analysis has demonstrated not only the dominance of male or patriarch-based societies, but culturally dominant societies, where the gendered demands (e.g., Western feminists) of one society are imposed upon other, less dominant societies. The bottom-up approach of feminist intersectionality is highly compatible with the usage-based perspective of cognitive linguistics.

Intersectional approaches have a logical place in the human security discussion, bringing the political "down" to the level of the individual, to bring a voice to the personal. The personal is political, and human security, with its focus on the individual, has the potential to support these personal voices. Discourses and practices are made visible – by looking within, through, behind (closed doors) and beyond the state, multiple actors come into view, those who are often marginalized when we only look at the state.

Risks: The overlapping competencies of team members (see 3.1) and the assignment of at least two point persons for each Work Package (see 3.2) reduces the risk that a Work Package could fail in the event that a team member is unable to carry out their tasks. The smaller size and different composition of the North Saami KORP corpus will impact the comparability of that data. THREAT-DEFUSER seeks to increase the contents of KORP in order to address this deficiency, primarily by increasing the number of newspaper texts. There is no known method that reliably distinguishes social media "likes" by humans from similar behavior produced automatically (by bots). However, monitoring by THREAT-DEFUSER will reveal sudden peaks and other unusual behavior that might contribute to distinguishing bots from human users.

2. Impact

2.1 Potential impact of the proposed research

THREAT-DEFUSER is the first cross-linguistic analysis of threat vocabularies and the Keywords/Keymorphs that show differential behavior in news media. We are the first to apply Normalized Social Distance metrics to the media sources of Russia and Norway. THREAT-DEFUSER contributes to UN sustainable development Goal 16: Promote just, peaceful and inclusive societies. This is achieved by ensuring public access to ratings of the ideological biases and audience exclusivity of news media, essential information that mitigates social fragmentation and radicalization. News media ratings are delivered via the NewsRadar app that alerts consumers alongside their news feeds.

2.2 Measures for communication and exploitation

The audiences of THREAT-DEFUSER include the scholarly communities of political scientists, linguists, media specialists, policy-makers, as well as all consumers of news media in the broader public. THREAT-DEFUSER will disseminate results in open-access scholarly journals in all three fields, and resulting datasets will be publicly archived, for example on the TROLLing (Tromsø Repository of Language and Linguistics https://dataverse.no/dataverse/trolling) platform. **Four conferences** will increase the visibility of this research and foster further interdisciplinary explorations inspired by THREAT-DEFUSER. The general public in Norway and Russia are served by a **project website**, a series of **podcasts** highlighting results, and the **NewsRadar app** that puts ideological and connectivity ratings at consumers' fingertips.

3. Implementation

3.1 Project manager and project group

The THREAT-DEFUSER team is a constellation of leading experts across the disciplines (political science, linguistics/language, media studies/computational approaches) and regions (Norway, Sápmi [Saami lands], Russia) of the project (see Table 1 on p. 7).

Janda and Nesset, who lead the Cognitive Linguistics: Empirical Approaches to Russian (CLEAR) research group at UiT, are prominent researchers in cognitive linguistics with a focus on Russian and analysis of corpus data. Janda's work (Janda & Clancy 2006) has informed the development of Keyword/Keymorph analysis. Janda and Nesset have spearheaded the conceptual design of numerous Internet resources for public use in Russian linguistics and language pedagogy, as well as the Tromsø Repository of Language and Linguistics. Gjørv is a leading scholar in security studies and in particular human security, citizen/civilian relations and activities in conflict with a focus on civil-military relationships and in population-centric and hybrid warfare scenarios. Her focus has been on human security perspectives in a variety of conflict scenarios and the importance of citizen/civilian agency in conflict. Trosterud is a pioneer in language technology for North Saami, ensuring the best possible corpus data and analysis for that language. Computational and programming expertise and web-development is provided by Radovan Bast, Senior Engineer in Digital Research Services at UiT. Cullen is an internationally-recognized expert in hybrid warfare. Benko, as leader of the Aranea project, guarantees that THREAT-DEFUSER has state-of-the-art multi-billion-word corpora for Russian and Norwegian, with powerful tagging, collocation, and word embedding functions. Cvrček (co-director of the Czech National Corpus) and Fidler are co-developers of Keyword/Keymorph Analysis and provide leadership for the development of parallel applications and analyses for Norwegian, North Saami, and Russian. Media studies expertise is covered by Pötzsch, Rogatchevski, and Šlerka, and the latter also oversees the implementation of social media tracking and measurement via Normalized Social Distance.

	Disciplinary Expertise			Regional Expertise		
Name, Affiliation	**PoliSci**	**Ling/Lang**	**Media/Comp**	**Norway**	**Sápmi**	**Russia**
Laura A. Janda, UiT (PI)		✓✓✓		✓	✓✓	✓✓✓
Radovan Bast, UiT			✓✓✓			
Gunhild Hoogensen Gjørv, UiT	✓✓✓			✓✓✓		✓✓✓
Tore Nesset, UiT		✓✓✓		✓✓✓		✓✓✓
Holger Pötzsch, UiT			✓✓✓	✓✓		
Andrei Rogatchevski, UiT		✓	✓✓✓	✓		✓✓✓
Trond Trosterud, UiT		✓✓✓	✓✓	✓✓✓	✓✓✓	✓✓
Patrick J. Cullen, NUPI	✓✓✓			✓✓✓		✓✓✓
Vladimír Benko, Slovak Academy of Sciences		✓✓✓	✓✓✓			✓✓
Václav Cvrček, Charles University		✓✓✓	✓✓			✓
Masako Fidler, Brown University		✓✓✓	✓✓			✓✓✓
Josef Šlerka, Charles University		✓	✓✓✓			✓

Table 1: THREAT-DEFUSER Team: Local shaded in yellow, National in green, International in blue
Key: ✓= competence, ✓✓ = competence/peer-reviewed publications, ✓✓✓ = high expertise/recognized international leader

3.2 Project organisation and management

Five Work Packages (WPs) integrate the THREAT-DEFUSER methods as shown in the Gantt chart on p. 8. Each WP is led by two Point Persons responsible for workflow, though all team members contribute.

WP1: Language of Threats; Point Persons: Gjørv, Janda & Fidler

WP1 combines social science and linguistic scholarship. A detailed literature review in hybrid warfare will be carried out, examining the trajectory of threat posturing emanating from different national sources, assessing how the term "hybrid warfare" became popularized and in which literature, how hybrid warfare has been represented across different national contexts (including Russian and Norwegian), and providing an initial assessment of dominant terminology in the literature (Norwegian, Russian, and English). WP1 accesses the largest comparable reference corpora with linguistic tagging that supports Keyword/Keymorph analysis. The Aranea Family of Gigaword Web Corpora (http://unesco.uniba.sk/aranea_about/) contains a Russian corpus, and Aranea leader Benko has constructed a Norwegian web corpus for the project with both bokmål and nynorsk varieties. UiT houses the KORP corpus of North Saami (http://gtweb.uit.no/korp), with full automatic tagging. WP1 develops "seed" vocabularies of words and collocations that are symptomatic of news articles/broadcasts that highlight threats. Seed vocabularies for each language will be enhanced by computational means such as the use of semantic vectors and word embeddings, as well as search engines that extract collocations (cf. Araneum functions and Collocations Colligations Corpora for Russian http://cococo.cosyco.ru). Threat vocabularies are enhanced by a feedback loop from text analysis in WP2.

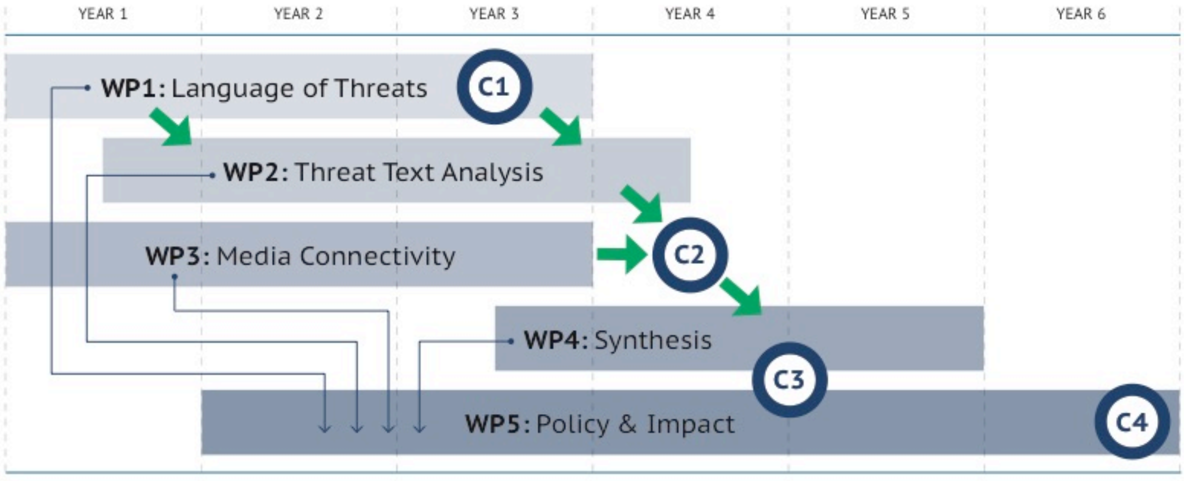

Figure 3: Gantt chart for THREAT-DEFUSER project (WP=Work Package, C=Conference)

WP2: Threat Text Analysis; Point Persons: Nesset & Cvrček

Seed vocabularies for Russian, Norwegian, and North Saami developed in WP1 supply search terms for the extraction of target texts and ensure that THREAT-DEFUSER will collect substantial samples of news from online newspapers, TV broadcasts, and podcasts that comprehensively reflect the landscape of threat-related discourse in each language. Russian TV broadcasts are currently captured by the UCLA NewsScape Library (http://tvnews.library.ucla.edu/) and publicly available for research. NewsScape capture includes closed caption texts that can be harvested for input into R and other analytical software. This capture now includes Russian pro-government channels (Pervyj, NTV, TVC). A capture station for Norwegian TV news will be set up and maintained at UiT and archived in NewsScape; we will attempt to set up capture also for the Russian opposition TV channel Dožd'. Newspaper, radio and other Internet portals will include an extensive range of options, such as mainstream (Aftenposten, NRK) and right-wing (Resett, Document) in Norwegian and North Saami (Ávvir, NRK-Sápmi); and opposition (Novaja gazeta, Vedomosti, Èxo Moskvy) and foreign (Radio Liberty, BBC Russian) in Russian.

THREAT-DEFUSER will develop Keyword/Keymorph analysis for Russian, Norwegian and North Saami by significantly enhancing the existing KWords application hosted at the Czech National Corpus portal (www.korpus.cz), improving robustness of the application, and adding language-specific settings. These improvements will consider copyright and other legislative restrictions in order to maintain free and unrestricted access to the tool for all users. With Keyword/Keymorph analysis for each language in place, we proceed to in-depth investigation of target text deviations from reference corpora in terms of both words and meaning-bearing grammatical categories. Here THREAT-DEFUSER reveals differential linguistic behavior that may be indicative of ideological slants and makes comparisons across media sources and languages.

WP3: Media Connectivity; Point Persons: Pötzsch & Šlerka

WP3 will critically interrogate the interface between civilian and media agency, and devise concrete strategies for communication, verification, and de-escalation with regard to perceived threats. These communication strategies will be simultaneously shared and tested with the other WPs. The spectrum of media sources in Norway and Russia and their audiences are probed for connectivity, tracked in terms of social media likes of news posts and measured in terms of Normalized Social Distance (Šlerka & Šisler

2017); Šlerka provides knowledge transfer to apply also to Russian social media (VKontakte, Odnoklassniki, moj mir). Media maps for each country are constructed and groupings of media sources are classified. In addition, this WP addresses processes and practices of escalation and radicalization in an extended security paradigm by investigating the intersecting dynamics of new media technologies (in particular social media and digital networks) and the mediation of perceived threats through populism and extremism. WP3 investigates the relationships between increasing global trends in populism and various expressions of agency through extremism in response to perceived threats. Relying on intersectional analysis (closely connected to feminist/gender analysis) we can better contextualize and understand the technological, economic, cultural, societal, and political patterns of support and restraint predisposing civilians' cognition and actions in encounters with perceptions of invisible threats. Addressing the role of civilians in contemporary media-fueled affective (emotional) politics in Western democracies, WP3 employs theories of trust and civilian capabilities/agency (informed by intersectional analysis) to understand the politicized roles of civilians in emerging crisis scenarios, with a particular focus on the role of media technologies, institutions, and practices in creating/maintaining/destabilizing environments that foster populism, and further various forms of extremism.

WP4: Synthesis; Point Persons: Gjørv & Trosterud

Results from WP1-3 come together in comparisons across languages, countries, and media, exposing trends and differences. Political implications are identified, and strategies are developed to address gaps in knowledge. Discourse analyses of central texts addressing hybrid threats (in Russian, Norwegian/North Saami, and English) will be conducted and triangulated with results from WP2 and 3 which will result in a multiple trajectory (quantitative and qualitative) knowledge base of key threat-oriented language used in various media. This knowledge base will serve as the foundation for WP5 and creation of the NewsRadar plug-in. WP 4 will use qualitative methods (surveys, participant observation, interviews) to gather data on how individuals in Norway, Sápmi, and NW-Russia actually receive, negotiate, and potentially repurpose or subvert allegedly radicalizing content disseminated in and through digital networks. This shift of focus on media practices takes seriously the agency of individual citizens and will help identify various machinic agencies interacting and interfering with human users. The WP will produce qualitative data sets on actual behavior with which assembled quantitative data sets on abstracted aggregates can be correlated to control for validity and reduce biases caused by selection of sources and other factors.

WP5: Policy & Impact; Point Persons: Bast & Cullen

Results from WP1-4 feed production of a webpage, podcast series, and policy advisories that disseminate results to the public and to policy makers. A component of WP5 will be to set up a sustainable model to assure that the website remains operative also beyond the end of the project. Additionally, the NewsRadar app/plug-in will be developed in Norwegian and Russian to break the "filter bubbles" by rating news media and offering alternative views classed according to results in WP4. This WP intertwines with the previous WPs, specifically targeting core stakeholders and potential end-users regarding current perceptions of invisible threats and how to manage these in a highly information-driven, digital-oriented/dependent society like Norway. In addition to connecting to stakeholders/end-users (business, NGOs/civil society organizations, unions, political parties, etc.) and establishing preliminary attitudes and perceptions amongst these actors, WP5 establishes an open debate/seminar forum for these and other relevant participants. The WP cooperates with UTSYN, an organization well connected to central, interested authorities (particularly within the foreign and defence policy communities), ensuring the visibility of THREAT-DEFUSER research and results to both policy actors and civil society. Debate/seminar results will be shared regularly with project partners, while WP5 will also ensure that academic publications will be regularly disseminated to general audiences through media outlets including editorials and commentaries. WP5 will manage all dissemination output, ensuring visibility as research is published. It will also manage inputs and responses, monitoring feedback by stakeholders and the general public to the ongoing research.

All WPs will yield multiple articles for publication in internationally-recognized (Cristin niveau 1-2) open-access scholarly journals across the three disciplines of the project, such as (political science:) *Stability: International Journal of Security and Development, Journal for Deradicalization, Journal of Eurasian Studies, Internet Policy Review*; (linguistics:) *Glossa, Journal of Applied Language Studies, Oslo Studies in Language, Open Linguistics*; (media studies:) *Journal of Information Policy, Media and Communication, JOMEC Journal, Social Media + Society*. THREAT-DEFUSER will host four conferences (C1-C4 in Gantt chart above): C1 on Threat Language and Texts, C2 on Threat Propagation Through Media Connectivity, C3 on Threats Across Languages and Cultures, and C4 on Defusing Threats Through Policy and Information. Relevant academic conferences include: International Studies Association, British International Studies Association, International Cognitive Linguistics Conference, Nordic Slavists Meeting, Slavic Cognitive Linguistics, Tension of Europe Conference, International Conference on ICT, Society and Human Beings. THREAT-DEFUSER will reach out to policy makers in the Directorate for Civil Protection (DSB), Ministry of Justice and Public Security, Ministry of Defence, and Ministry of Foreign Affairs, in addition to those at the municipality level, particularly in Tromsø kommune, Kirkenes, and Kautokeino. Media coverage will be sought in local, national, and international channels such as *NRK Sápmi, Aftenposten, Nordlys,* and *The Independent Barents Observer*.

Conclusion

Using quantitative analysis of digitally networked communication and reassessing the acquired data through qualitative approaches, THREAT-DEFUSER identifies the role of disinformation in technologically facilitated dynamics of radicalization. We determine the function and possible effects of these dynamics in contemporary hybrid warfare, and develop concrete evidence-based recommendations for reduced vulnerability and increased resilience of societies and political systems in relation to such incursions.

References

•Ackerly, B. A., M. Stern, J. True (2006). Feminist methodologies for International Relations. Feminist Methodologies for International Relations. B. A. Ackerly, M. Stern and J. True. Cambridge, Cambridge University Press: 1-15. •Baisa,V., O. Herman, A. Horák. (2017). Manipulative Propaganda Techniques Technical Report. In: Aleš Horák, Pavel Rychlý, Adam Rambousek (Eds.): Proceedings of Recent Advances in Slavonic Natural Language Processing 2017, pp. 111–118, 2017. •Baker, P. (2004). Querying Keywords: Questions of Difference, Frequency, and Sense in Keywords Analysis. Journal of English Linguistics, 32(4), 346–359. https://doi.org/10.1177/0075424204269894 •Baker, P. (2006). Using Corpora in Discourse Analysis. London; New York: Continuum. •Baker, P., & McEnery, T. (2005). A corpus-based approach to discourses of refugees and asylum seekers in UN and newspaper texts. Journal of Language and Politics, 4(2), 197–226. •Benko, V. Aranea: Yet Another Family of (Comparable) Web Corpora. In *Petr Sojka, Aleš Horák, Ivan Kopeček and Karel Pala (Eds.): Text, Speech and Dialogue. 17th International Conference, TSD 2014, Brno, Czech Republic, September 8-12, 2014. Proceedings. LNCS 8655.*Springer International Publishing Switzerland, 2014. pp. 257-264. ISBN: 978-3-319-10815-5 (Print), 978-3-319-10816-2 (Online). •Benko, V. & V. P. Zakharov. 2016. Very Large Russian Corpora: New Opportunities and New Challenges. Computational Linguistics and Intellectual Technologies: Proceedings of the International Conference "Dialogue 2016" Moscow, June 1–4, 2016 http://www.dialog-21.ru/media/3383/benkovzakharovvp.pdf •Blatt, B. 2017. *Nabokov's Favourite Word is Mauve.* London: Simon & Schuster. •Cavelty, M. D., M. Kaufmann and K. S. Kristiensen (2015). Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue* 46(1): 3-14. • Chandler, D. and J. Reid (2016) *The Neoliberal Subject: Resilience, Adaptation and Vulnerability.* London: Rowman and Littlefield. •EuropeAid (2016). Building Resilience: The EU's approach. EU FACTSHEET: Humanitarian Aid and Civil Protection Development and Cooperation. •Fearon, J. D. (1994). Domestic Political Audiences and the Escalation of International Disputes. *The American Political Science Review* 88(3): 577-592. •Firth, J.R. 1957. A synopsis of linguistic theory. Studies in linguistic analysis, Blackwell, Oxford. •Fidler, M. & V. Cvrček. 2018. Going Beyond "Aboutness": A Quantitative Analysis of Sputnik Czech Republic. In M. Fidler, V. Cvrček (eds.), *Taming the Corpus, Quantitative Methods in the Humanities and Social Sciences*, 195-225. https://doi.org/10.1007/978-3-319-98017-1_10 •Gray, G. C. (2017). Academic Voice in Scholarly Writing. *The Qualitative Report* 22(1): 179-196. •Heffington, C. (2017). Marked Targets: Coercive Diplomacy and Domestic Terrorism. *Journal of Global Security Studies* 2(2): 123-136. •Hoogensen, G. & S. V. Rottem (2004). Gender Identity and the Subject of Security. *Security Dialogue* 35(2): 155-171. •Hoogensen Gjørv, G. (submitted). Civilian agency in conflict: protection vs resilience? *Journal of Global Security Studies*. •Janda, L. A. 2015. Cognitive Linguistics in the Year 2015. *Cognitive Semantics* 1, 131-154. •Janda, L. A., & S. Clancy. 2006. *The case book for Czech*. Bloomington, IN: Slavica. •Jose, B. and P. A. Medie (2015). Understanding Why and How Civilians Resort to Self-Protection in Armed Conflict. *International Studies Review* 17(4): 515-535. •Keating, M. and D. Della Porta (2010). In defence of pluralism in the social sciences. *European Political Science* 9: S111-S120. •Křen, M., Cvrček, V., Čapka, T., Čermáková, A., Hnátková, M., Chlumská, L., et al. (2016). SYN2015: Representative Corpus of contemporary written Czech. In N. Calzolari, K. Choukri, T. Declerck, S. Goggi, M. Grobelnik, B. Maegaard, et al. (Eds.), *Proceedings of the tenth international conference on language resources and evaluation (LREC'16)* (pp. 2522–2528). Portorož, Slovenia: ELRA http://www.lrec-conf.org/proceedings/lrec2016/index.html. •Krüger, Uwe. (2016). *Mainstream - Warum wir den Medien nicht mehr trauen*. Munich: C.H. Beck. •MacLeod, Alan. (2019). Chavista 'thugs' vs. opposition 'civil society': western media on Venezuela. *Race and Class*. https://doi.org/10.1177%2F0306396818823639 •Mosteller, F. & D. L. Wallace. (1963). Inference in an Authorship Problem. *Journal of the American Statistical Association* 58: 302, 275-309. •Reichborn-Kjennerud, E. & P. Cullen (2016). What is Hybrid Warfare? Policy Brief. Oslo: Norwegian Institute of International Affairs. •Singer, P. W. & E. Brooking. (2018). *LikeWar: The Weaponization of Social Media*. Boston: Houghton Mifflin Harcourt. •Šlerka, J. & V. Šisler. 2018. Charles: Who is shaping your agenda? Social network analysis of anti-Islam and anti-immigration movement audiences on Czech Facebook. In: Kristian Steiner and Andreas Onnerfors (eds.), Palgrave Macmillan, 61–85. •Scott, M., & Tribble, C. (2006). Textual Patterns: key words and corpus analysis in language education. Philadelphia: John Benjamins. https://doi.org/10.1075/scl.22 •Sørensen, H. & D. B. Nyemann. (2018). Going Beyond Resilience: A revitalised approach to countering hybrid threats. *Strategic Analysis* November 2018. Helsinki: Hybrid CoE.