ICONO 14, Revista de comunicación y tecnologías emergentes
ISSN: 1697-8293
info@icono14.net
Asociación científica ICONO 14
España

Freedman, Jane; Hoogensen Gjørv, Gunhild; Razakamaharavo, Velomahanina
Identity, stability, Hybrid Threats and Disinformation
ICONO 14, Revista de comunicación y tecnologías emergentes, vol. 19, no. 1, 2021, -June, pp. 38-69
Asociación científica ICONO 14
España

DOI: https://doi.org/10.7195/ri14.v19i1.1618

Available in: https://www.redalyc.org/articulo.oa?id=552565288003

MONOGRAPH

Identity, stability, Hybrid Threats and Disinformation

Identidad, estabilidad, amenazas híbridas y desinformación

Identidade, estabilidade, ameaças híbridas e desinformação

Jane Freedman
Professor
(Université Paris 8)
https://orcid.org/0000-0002-0011-6164
France

Gunhild Hoogensen Gjørv
Professor
Critical Studies on Peace and Conflict
(UiT The Arctic University of Norway)
https://orcid.org/0000-0001-8037-7796
Noruega

Velomahanina Razakamaharavo
Visiting Fellow
(Technical University Munich)
https://orcid.org/0000-0002-0051-9190
Germany

Reception date: 31 August 2020
Review date: 1 September 2020
Accepted date: 9 December 2020
Published: 1 January 2021
To cite this article: Freedman , J., Hoogensen Gjørv, G. & Razakamaharavo, V. (2021). Identity, stability, Hybrid Threats and Disinformation, *Icono 14, 19*(1), 38-69. doi: 10.7195/ri14.v19i1.1618

MONOGRAPH

Abstract

The following article examines the relevance of gender and intersectional analyses to better understanding hybrid threats, in particular those that are increasingly targeting civilian environments. The authors first present relevant concepts including hybrid threats and warfare, resilience, disinformation, civilian agency, and intersectionality as a method. Thereafter they discuss how disinformation is used to destabilise societies by directly attacking civilian spaces and attempting to foment polarisation and unrest, if not conflict. The authors then discuss how the concepts of disinformation and civilian agency are illuminated through gender and intersectional analyses, speaking to complex, civilian contexts by examining how gender (and race) have been employed to attempt to foment destabilisation. They conclude with some brief reflections about the role of gender and intersectional approaches in understanding hybrid threats and warfare, not just in Europe but also for other parts of the world.

Key Words: *Hybrid threats; Disinformation; Gender; Intersectionality; Destabilisation; Identity*

Resumen

El artículo examina la relevancia de los análisis interseccionales y de género para comprender mejor las amenazas híbridas, en particular aquellas que se dirigen cada vez más a entornos civiles. En primer lugar se presentan los conceptos más relevantes, que incluyen: amenazas híbridas y guerra, resiliencia, desinformación, agencia civil e interseccionalidad como método. A partir de estos, se discute cómo se utiliza la desinformación para desestabilizar sociedades atacando directamente los espacios civiles e intentando fomentar la polarización, el malestar o directamente el conflicto. A continuación, se discute cómo los conceptos de desinformación y agencia civil se pueden comprender a través de análisis interseccionales y de género, cuando se abordan contextos civiles complejos al examinar cómo se ha empleado el género (y la raza) para intentar fomentar la desestabilización. Las conclusiones proponen algunas breves reflexiones sobre el papel del género y los enfoques interseccionales en la comprensión de las amenazas híbridas y la guerra, no solo en Europa sino también en otras partes del mundo.

Palabras clave: *Amenazas híbridas; Desinformación; Género; Interseccionalidad; Desestabilización; Identidad*

Resumo

O artigo examina a relevância das análises intersetoriais e de gênero para entender melhor as ameaças híbridas, particularmente aquelas que têm como alvo cada vez mais ambientes civis. Em primeiro lugar, são apresentados os conceitos mais relevantes, que incluem: ameaças híbridas e guerra, resiliência, desinformação, agência civil e interseccionalidade como método. Com base nisso, discute-se como a desinformação é usada para desestabilizar as sociedades, atacando diretamente os espaços civis e tentando promover a polarização, a agitação ou o conflito direto. A seguir, é discutido como os conceitos de desinformação e agência civil podem ser entendidos por meio de análises intersetoriais e de gênero, ao abordar contextos civis complexos, examinando como gênero (e raça) tem sido usado para tentar promover a desestabilização. Os resultados propõem algumas reflexões breves sobre o papel do gênero e das abordagens intersetoriais na compreensão das ameaças híbridas e da guerra, não apenas na Europa, mas também em outras partes do mundo.

Palavras chave: *Ameaças híbridas; Desinformação; Gênero; Interseccionalidade; Desestabilização; Identidade*

1. Introduction

Current analyses of hybrid threats pay very little attention to gender or the intersection of different identity markers as an element of analysis (a recent exception being Herrero-Diz et.al 2020). This is typical of more traditional approaches to threats and warfare that are generally state-centric and show less awareness of the role of the civilian domain to the dynamics of conflict. Understanding hybrid threats and warfare, however, reveals the complex spectrum of conflict that recognises multiple approaches (beyond military) to create destabilisation, insecurity, and eventually violent conflict. More recent research on hybrid threats explores the roles of civilians in the hybrid threat and conflict spectrum, and in particular how non-military tools are employed to disrupt and destabilise the civilian environment, having broader implications on local, regional and national

security (Hoogensen Gjørv 2020). To better understand how civilians are actors as well as targets in hybrid warfare scenarios, it is crucial to understand the civilian domain itself, and where its potential vulnerabilities lie. These vulnerabilities are often connected to identity markers that intersect in various social contexts, from gender and class to race, ethnicity, age, and sexual orientation. These markers are integrally linked to societal social norms roles, and beliefs that are crucial to what civilians consider fundamental to the survival of their physical or social selves. In other words, to their and societal and national survival and security.

We argue that including an intersectional analysis is thus relevant to identifying vulnerabilities in society, but is also instrumental to understanding the possibilities for societal resilience – the ability of society to resist or respond to hybrid threats. As such, gender and other intersecting identity markers are important both in understanding the risks posed by hybrid threats, their potentially different impacts on men and women (often combined with other identity markers such as race/ethnicity or sexual orientation, for example), and the ways in which resilience can be strengthened. This paper will review how we understand hybrid threats and the role civilians play in the transmission of such threats, and then propose an overview of the ways in which gender and intersectional analysis can be better used in relation to analysis of hybrid threats, using examples from recent incidents in Europe, to strengthen understanding and provide more comprehensive recommendations for building resilience.

Before going on to analyse the ways in which gender is important in hybrid threats and resilience, it is important to define exactly what we understand by hybrid threats and resilience. The term hybrid threat or hybrid warfare has been criticised for lack of analytical clarity, and it is clear that it can encompass a wide variety of different elements.

2. Method

In this paper we apply a concepts-oriented approach to case examples to demonstrate how gender and intersectionality are relevant and important in our understanding of how hybrid threats operate in the civilian domain. As such we first

elucidate what we mean by gender and intersectionality, lenses through which we argue we can better understand the strengths and vulnerabilities of the civilian domain in the context of hybrid threats and warfare. We then present the core concepts we will work with, both defining these concepts but initially flagging gender and intersectionality as we do so. We focus upon the concepts of hybrid threats, resilience, disinformation, civilian agency and, and thereafter engage these concepts in the Development section with regard to the destabilisation of societies, and the potential of resilience informed by gender perspectives.

2.1. Gender, intersectionality, and the complexity of the civilian environment

Discussions about how we understand gender continue to evolve. In the 1980s and 1990s it was increasingly clear that a lot of the work addressing gender inequalities – generally pertaining to inequalities between men and women - nevertheless excluded certain, marginalized, segments of the female population, namely women of colour and/or of non-European ethnicities. It became increasingly recognised that it was not enough to speak about "women" in general, because even between women many different inequalities existed on the basis of race, ethnicity, sexual orientation, class, and other identity markers. Thus the term "Intersectionality" was introduced to take into account the complexity of inequalities and power relations between not just binary and simplistic, categories of "men" and "women", but between different classes of white women (affluent or middle class, or working class or poor), or between white and black or brown women, women of European heritage (often characterised as "white" and "christian") and women of colour and/or outside of the Christian tradition (including indigenous women), which could be even further complicated by class, sexual orientation, or other marginalized identities.

Coined by Kimberlé Crenshaw in the late 1980s (Crenshaw 1991), the term *intersectionality* was designed to critically assess the intersection between race, gender, class and other identity categories that have been regularly produced and reproduced within different contexts. Intersectional analysis makes visible how identity has been produced and used to expand, reinforce, or reduce power. As not-

ed by Mohanty, "focusing on the identities and perspectives of the marginalized can produce a deeper knowledge of objective social structures and their effects… [Theories] elaborated through such concepts as "intersectionality" and "epistemic privilege" – are based on a non-positivist conception of objective social knowledge" (Mohanty, 2018: 418). In an interview Crenshaw noted (Coaston 2019) that this approach has been subjected to a backlash, being accused of creating "identity politics," and is itself responsible for fragmenting societies along identity lines, in turn creating mistrust and distrust between people. Such accusations reflect what we will continue to examine below: systems of trust have often relied upon, and studied through, the normalisation of an assumed "identity-free" universal man (Yuval-Davis, 2011). When challenged however, the universal man is exposed as reflecting the identities of those with power in a given society (eg: affluent, white, male, able, heterosexual) (Carasthatis, 2014). Those not reflecting these normalised identities become threats to that system of trust. Indeed, for that system to survive, distrust of the other (identity) is imperative (Bilgic, Hoogensen Gjørv & Wilcock 2019). As agents of security, states can try to build or maintain institutional trust through particularised distrust-building towards the racialised, gendered, classed "other".

The dynamics behind hybrid threats (discussed below) demonstrate the complexities of the various ways gender and other identity markers can be defined and manipulated to serve specific purposes. Gender is a relational concept whose construction varies across geographical space and time. The impacts of gender constructions are to be understood in relation to other socially constructed categorizations and hierarchies of power such as race and class. The conceptualization and definition of gender are highly fluid and dynamic depending on the intervening events and actors taking part in the construction process. Gender categorisations can be manipulated and refashioned in discourses, instrumentalized in politics, or reconstructed by individuals and communities to target social vulnerabilities. Hybrid threats such as the examples that follow in this article show the extent to which gender is complex and intersects with other identities. In situations involving threats that focus on the identities of (usually) marginalized or non-dominant identities (Hoogensen and Stuvøy 2006), the identity of the other is constructed by the self as abnormal, not fitting into the dominant group, different, not trust-

worthy, a threat and thus he/she/ they must be punished, sent to jail or back to his/her/ their homeland(s) etc. These constructions of the other as a threat are based on the manipulation of social norms that there are "normal" or "traditional" gender norms and behaviours which these "others" threaten. A typical example (also illuminated by Crenshaw above) is the backlash against a perceived undermining of "natural" masculine dominance by feminists who call for gender equality. Societal vulnerabilities and particularly those associated with polarizations and misunderstanding on gender issues can be exploited through hostile campaigns employing digital communication. For example, online, with micro-targeting and social engineering, it is very easy for malevolent actors to target a massive number of civilians on social media and in video games using Augmented Reality (AR) and Virtual Reality (VR) diffusing messages making use of fabricated/ imagined/ constructed "identities" that are further labeled as a threat and engaging in vile, malevolent, and criminal acts. Such malevolent actors use specific tropes or stereotypes exploiting identities/differences/ inequalities that are present as existing social cleavages. If the disinformation begins with a focus on gendered discourses, the public can easily shape, refashion, and extend the disinformation so that other identities are targeted, enacting civilian agency.. Communities that are sympathetic to the messaging of the original disinformation often rely on the particularized trust (Bilgic, Hoogensen Gjørv & Wilcock 2019) that reverberates and grows within social echo chambers (often on social media), thus strengthening their own perceptions of their selves (the pure, the natives, the high people, the victims of threats, the innocent white young women etc.) and sustaining divisions, othering, discrimination, exercise of one's power and dominance over the other.

Using this framework helps us to understand the ways in which political cleavages or vulnerabilities operate, and further how they are targeted through hybrid attacks.

2.2. Hybrid threats and warfare

There continues to be debate around the definitions about hybrid warfare, hybrid threats, and a related concept "gray zone" conflicts. There is additionally an overlap or conflation with other concepts such as remote warfare, asymmetric

warfare, new wars, sixth-generation/ contactless/ next-generation/ ambiguous/ asymmetrical/nonlinear warfare, full-spectrum conflict, among others (Watts & Biegon,2019; Giannopoulos et.al 2020).

Earlier conceptions of hybrid warfare maintained a kinetic or lethal component defining it as: "Threats that incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder, conducted by both sides and a variety of non-state actors" (Hoffman 2007: 8). As noted by James Wither (2016), this type of "hybrid" warfare was distinct from historical forms of warfare due to the mixing of methods – that is, conventional and irregular. However, the increased use of information warfare and targeting of public opinion became another distinguishing feature by 2014, as articulated by then NATO Secretary General Anders Fogh Rasmussen in his characterization of Russian tactics in Ukraine, focusing in part on what he called the Russian "aggressive program of disinformation" (Wither 2016: 76). In time, non-military methods of hybrid warfare, especially disinformation campaigns and other approaches to destabilize societies (such as cyber-attacks on infrastructure) have become key features of hybrid warfare and threats.

At the same time, the notion of "grey zone" conflicts have been increasingly used, referring to the blurring of the previously perceived lines between peace and war, where the latter manifested itself through the clear use of overt violence, often by state actors/militaries. The grey zone speaks to those measures that create destabilization and conflict below those thresholds we traditionally associate with war, the overt use of violence. Frank Hoffman distinguishes between hybrid warfare and grey zone conflicts whereby the latter is defined as "[t]hose covert or illegal activities of non-traditional statecraft that are below the threshold of armed organized violence…as a part of an integrated design to achieve strategic advantage" (Hoffman 2018: 36), which include disruptive tactics such as influence operations, disinformation, psychological operations, destabilizing legal processes, etc. This is contrasted with hybrid warfare which pertains more so to the "fused mix" of conventional weapons, terrorism, crime, and other forms of violence to "obtain desired political objectives" (ibid: 38). In other words, hybrid warfare is

not necessarily under threshold, and includes the use of violence. Hoffman notes that NATO employs a definition that is broader in scope, "depicting [hybrid warfare] as a mixture of military means with non-military tools including propaganda and cyber activity" (ibid: 39), which is closer to Hoffman's definition of grey zone conflict.

A considerable amount of research on hybrid threats and warfare focuses on state actors as perpetrators, as well as primary targets – addressing Russian tactics in the Baltic states, especially Ukraine (Fox & Rossow, 2017; Haynie, 2020; Veebel, 2020), the role of China (Raska, 2015, Burgers & Romaniuk, 2016), or the roles of NATO (Brânda & Sauliuc, 2020), the EU (Zaliznyak; 2016; Bajarūnas, 2020), and the US (Batyuk, 2017). Recent definitions of hybrid threats and warfare note that these strategies are dominantly employed by authoritarian states against democratic states (Giannopoulos et al 2020), even though the US has been accused of conducting hybrid activities against Russia and Iran, for example (Carden 2017; Ghaffari 2019). Non-state actors also present as aggressors, including groups classified as terrorists (Mumford, 2016) especially ISIS (Beccaro, 2018). Both the statecentric as well as terrorist-oriented focus explains what can be perceived as the significant amount of scholarship on hybrid threats/ warfare using mostly realist frameworks (Filipec, 2019; Muradov, 2019) They use the state as a security referent thereby downplaying or ignoring the roles other actors such as civilians, and the role ordinary people play in the ways conflict develops. The result has been that less consideration has been put on the importance of civilians (with the exceptions of a few scholars such as Bartowski, 2015; Ratiu & Munteanu, 2018; Hoogensen Gjørv 2017; Hoogensen Gjørv & Bilgic, forthcoming) along with the implications of gender and other intersectional identity markers in the resulting security dynamics.

In an EU Commission Joint Research Centre (JRC) Technical Report, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) highlights the use of the term "hybrid threat" as an umbrella concept, and notes that in particular it "raises the issue of systemic vulnerabilities of democratic systems as particular targets" (Giannopoulos et al 2020: 1). The report therefore focuses on hostile actors that target vulnerabilities in democratic states, using tactics asso-

ciated with authoritarian or rogue states and non-state networks. They use then "multiple synchronized tools (in principle non-military)", create ambiguity (hiding intent and attribution), and often include a distraction element (ibid: 2). To understand hybrid threats one needs to understand the actors, tools, the domains that are targeted and the phases of attack (ibid: 3). Hybrid warfare falls within this spectrum of activity as the "hard end" of hybrid threat activity (ibid: 33). This approach resembles therefore a mix of the hybrid warfare and gray zone conflict approaches outlined above, though hybrid threats are the rough equivalent of grey zone conflict (and under threshold, or before the exercise of overt violence), and hybrid warfare is distinctly separate resembling Hoffman's definition of hybrid warfare and the employment of violence and/or traditional military measures. Julian Lindley-French, who has written extensively on NATO, draws on the concept of "maskirovka" (military deception) employed by Soviet forces in WWII. Lindley-French defines maskirovka as "war that is short of war, a purposeful strategy of deception that combines use of force with disinformation and destabilization to create ambiguity in the minds of Alliance leaders about how best to respond" (Lindley-French 2015: 4 in Wither 2016: 82). For the purposes of our article we focus in particular upon the under threshold (grey zone) activities as these are in particular relevant to the targeting, manipulation, and cooperation within the civilian domain. It can be argued that better preparation to meet hybrid threats/grey zone conflicts will mitigate the necessity to employ violent means in an escalated hybrid warfare scenario.

Though there is no clear agreement on a definition (Reichborn-Kjennerud/Cullen 2016), we can characterize features as such: 1.Employs a combination of multiple means including military, political, economic, legal, cultural, social, infrastructure, cyber and information domains; 2. A hostile actor aims to avoid detection and tries to diffuse/confuse the situational awareness; 3. A hostile actor can be state, nonstate or proxy actors (or all of them); 4. It tries to create a situation where existing societal differences and grievances are exacerbated. This is especially done in the civilian domain by non-military means, both cyber-attacks (on infrastructure, for example) or by disinformation campaigns.

2.3. Resilience

The impact and breadth of hybrid threats provides a lot of insight into how people, communities and nations handle a crisis or conflict. It tests the resilience of a society, and illustrates the degree to which societies can be destabilized by a non-military threat. Article 3 of the NATO Treaty addresses resilience, with the expectation that each member state resists armed attack on the basis of "their individual and collective capacity." Resilience is understood as "a society's ability to resist and recover easily and quickly from such shocks and combines both civil preparedness and military capacity" (NATO 2020).

Much of a society's resilience lies in its population and people's abilities to respond to a crisis, and perhaps more importantly, people's abilities to adapt to abrupt and potentially long-lasting change.

Resilience reflects an ability to "bounce back" and tackle a crisis and/or threat, but also an ability to evolve or adapt. Assumptions about resilience are evident in narratives about "returning back to normal" after the coronavirus crisis. Such assumptions do not take into account how changes themselves may become normalized over time, and how attitudes and behaviours – not least amongst citizens - change as a result. People expect governments to solve a crisis as soon as possible. But what if, like in the coronavirus crisis, that is not possible? Resilience in society may demand adjustments to "new" normal, including new perceptions of insecurity.

2.4. Disinformation

Disinformation has attracted significant interest from various disciplines, (media and communication, political science, psychology, science and technology studies, etc.). Some scholars work on the motives and intents behind the mechanisms or tools used to spread the information. Little is still known, however, about the role of the targets of disinformation – civilians – and their reactions to disinformation, and the subsequent effects of these on security dynamics in various contexts. Disinformation is a contested concept (Derakhshan & Wardle 2017:

27), very often conflated with misinformation, which is wrong information, but not combined with a political motive to mislead and exacerbate social vulnerabilities. "Fake news", fabricated/manipulated content, rumors, information pollution, "malinformation", information disorder, junk news, propaganda and others are usually conflated with disinformation (Shu et al 2020). Fake news is "information deliberately fabricated and published with the intention to deceive and mislead others into believing falsehoods or doubting verifiable facts,"[1] and is linked to disinformation, misinformation, and malinformation (Shu et al 2020). Fake news "is misleading, in much the same way that disinformation is misleading: it is 'likely to create false beliefs'" (Gelfert 2018: 104). Disinformation is defined as "information that is false and deliberately created to harm a person, social group, organisation or country."[2] It targets and exploits socio-cultural cleavages with the intention of "creating social tension, polarising society, instilling fear in the population or undermining their trust in government" (Giannopoulos et al 2020: 43). In elections, fake news and other disinformation strategies are employed to cause confusion and harm including using myths, rumours, superstition (Shu et al 2020). Very often, civilians are not aware the information they share is "fake news" and fabricated with the intention to harm (to foment doubt and mistrust). Importantly, the spreading of misinformation or disinformation does not happen in a vacuum. Attempts to influence a society start with targeting existing vulnerabilities, and indeed, some sources of mis- and disinformation may not even try to disguise or hide themselves, as certain citizens may already be inclined to trust such sources and spread them willingly to promote a political agenda they support. As such, mis- and disinformation attacks may only require small scale or lightweight influence operations through selected media sites, which may be well-known and even popular. We need to be cognizant that mis- and disinformation can, as a result, be hidden in plain sight.

The rapid technological evolution accompanying advances in disinformation makes it important to better understand it. The literature has thus far examined the roles of various technologies in disinformation including bots, (software application running automated tasks (scripts)), botnets (Internet-connected devices, each running one or more bots) and AI, and the platforms they target such as social media like Twitter, WhatsApp, and Facebook. AI enhances the capability of other

technologies, (e.g. social media), and is generally understood as a technology, or an artificial system, imitating humans or reproducing human cognition using a large training dataset. There are many types of AI techniques (and applications): Artificial Neural Networks (ANN, e.g.: voice recognition), Generative Adversarial Learning (GAN, e.g.: generating photographs of human faces), Natural Language Processing (NLP, e.g.: predictive texts). In information operations targeting elections, some AI techniques are associated with threats: for example, the use of machine learning to conduct user profiling and micro-targeting exploiting big data, or the manipulation of audio and visual materials using GAN for "deepfakes". A significant gap in knowledge therefore is understanding how those technologies interact, influence each other and are used simultaneously, (and combined with offline practices, e.g. word-of-mouth) in disinformation, and the extent to which the information communicated with AI play and important role in disinformation affecting civilians, (e.g.: memes, images, voice and video deepfakes).

2.5. Civilian agency

Citizen actors engage in diverse strategies to ensure human security (physical and economic security primarily), ranging from cooperation with armed groups (state or non-state), selective sharing of information and resources, the spread of dis/misinformation, to everyday forms of resistance (Hoogensen Gjørv & Stuvøy 2006). Civilian 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). Civilian agency includes all activities approaching (but not including) the use of violence if conflict drivers amongst citizens are excessively aggravated (Heffington 2017). What then does citizen agency look like in different contexts? How has it affected the progression or regression of conflicts? Finally, how can understanding citizen agency better help move states and non-state actors out of conflict?

Citizen actions range from efforts to avoid physical violence, remain neutral, or be cooperative or collaborative (Baines and Paddon 2012). These actions are often influenced by trust levels between civilian and authorities, as well as impact trust levels within their communities/societies. The concept of civilian agency politi-

cises civilian roles by acknowledging potential power at the individual level, and using it towards either stability or instability. Very little is known about the importance of ordinary people in those dynamics especially in the contexts of hybrid threats. Civilian agency is integral to the assumptions hostile actors have about the potential to spread information - that people *will* spread it, and that they will be party to potential destabilization tactics, either unknowingly or unwillingly, or in fact, as sympathisers to the political agenda that the spread of such information could promote.

3. Development

3.1. Targeting civilians, reducing trust and increasing destabilisation

A primary concern resulting from waning trust in governance institutions is the potential for increased societal instability. Potential future crises in Europe will be dominated by a complex, hybrid form of challenges or threats that affect or target populations, in turn creating instability (Major and Mölling 2015, O'Loughlin 2015, Giegerich 2016, Lanoszka 2016). Citizen trust, loyalties, values, and politics are central to understanding these challenges to stability. Sustainable and legitimate governance relies upon trust between government institutions and their citizens, and sustainable government is weakened if trust is weak. Destabilisation - of states, governance structures, and societal relations - provides a crucial lens through which the impacts of trust can be analysed and measured, and helps us reappraise definitions and approaches to trust, including which levels are conducive to stable, sustainable and fair social relations and thriving citizens. It is also a lens through which we can analyse the ways in which waning trust influences governance.

Political stability pertains to the maintenance of expectations around the flow of political exchanges (Ake, 1975). Exchanges are political insofar as they affect, or try to affect, "the distribution of power to make decisions for that society" (ibid: 271). Laws and political roles contribute to the political structure in which such exchanges take place. Instability takes place when the political structure

is challenged, either by contesting roles or defying the law (for example). These challenge the authority of the political structure. As such, the degree to which a political structure can withstand such challenges, the more resilient the structure is. Destabilising actions can arise in the face of existing vulnerabilities – erupting from economic difficulties such as job losses, the spread of misleading and/or false information, fears of migration, increasing threats and consequences due to climate change, and so forth. Destabilisation has been directly linked to decreased trust in government institutions (European Commission 2018). Destabilisation is a result of purposeful action on the part of those who wish to affect the distribution of power in a society – the question is often whether these actions are internally driven or external. Often, it is a combination of both, whereby internally driven vulnerabilities become manipulated by external actors.

Destabilisation can occur due to a combination of forces to attempt to change the efficacy/power of the political structures/system in a society and state. The system itself may already create vulnerabilities if it is considered illegitimate by the people it is intended to rule – bottom up actions by some citizens to disturb and disrupt the political structure if it is seen as not representative of certain ideologies or politics may occur – including protests (that can turn violent – ie: yellow vests), media campaigns (influence information), the use of violence (terrorism), etc. Today there is an increasing awareness that the vulnerabilities of certain political systems, whereby legitimacy is already contested on one or more fronts, are further being manipulated by outside sources (state and non-state) to create even more instability. The concept of stability has experienced an awkward relationship with democracy. Moves towards more stability – through top-down governance measures – may hinder democracy rather than promote or support it. Democracies are considered to be significantly vulnerable to both internal as well as external disruptions and as they are particularly prone to vulnerabilities of legitimacy (Ülgen 2016). As comparatively less rigid and dominant as authoritarian systems that engage the use of force more readily to quell uprisings or discontent, democracies are more easily vulnerable to unrest, both that which arises from within, but also that which is manipulated from external forces. At the same time, it has been argued that democracies are better placed "to signal intentions and credibly to commit to courses of action in foreign policy than non-democracies"

due to the role of "audience costs" and the ability of citizens to articulate their support or rejection of governance institutions (Fearon 1994: 578).

The resilience of a society is heavily dependent upon the trust in which its citizens endow upon its institutions and governance approaches. The concept of resilience has been recently adopted by the EU as well as NATO as a response to destabilisation. In the EU context, resilience has been frequently associated with foreign and humanitarian aid initiatives. 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). 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 and Nyemann, 2018: 2).

In policy and scholarly literature, the focus on destabilisation have been largely on institutional responses, whereby EU and partners (eg: NATO) work towards strengthening responsiveness and preparedness of institutions and infrastructure so that they are less vulnerable to disruption and instability. Whether destabilising actions are internally or externally generated, the response largely relies on a central "solution", that is, resilience of societies and their institutions and infrastructures. The focus has been very top-down, where institutions are strengthened, and these strengths are passed along to citizens in the form of advice and guidance when confronted with crisis and instability. Far less however has been done to examine the role of civil society and citizens themselves, and how they can impact the potential "resilience" of institutions and infrastructures. Citizen action, inaction, or resistance for that matter, needs to be assessed as well, as they are a part of the social network that is expected to handle and overcome crisis and instability. In this respect therefore, trust is a crucial element in the role of citizen and/or civil society resilience.

A significant gap exists between institutional preparation and governance, and awareness of citizen agency, as resilience has focused on a top-down, institutional approach, strengthening primarily institutional structures against instability (EU, NATO, individual states). They fail to integrate insights into "security as resilience" understood as a bottom-up, citizen-oriented perspective (human security) through citizen agency (Chandler 2012). As well, citizen agency as resilience and trust is inadequately understood (Clark-Kazak 2014, Cavelty, Kaufmann et al. 2015, Jose and Medie 2015). Local behavioural patterns in this context are often subtle and relatively passive, and thus risk being overlooked by institutional approaches (Mac Ginty 2010: 403). Resilience practices of citizens may also be contradictory and inconsistent with institutional resilience strategies and expectations of trust (Cavelty, Kaufmann et al. 2015).

3.2. Looking at gender and intersecting identities: how are they relevant for thinking about hybrid threats?

As they combine the simultaneous employment of military and non-military tools, primarily targeting societies at large, hybrid threats cannot be countered solely by military means. In fact, below threshold (non-state violence), grey zone threats require an equally, if not more substantial and inclusive response from the civilian domain, and a strengthening of social trust and resilience among citizens. Gender and other identity marker divisions and hierarchies are a feature of all societies, so to provide an inclusive response we need to think about gender and the intersectional ways in which women and men coming from dominant or marginalized communities might be targets for or actors in hybrid threats.

Gender is one of the most central identity markers, and lenses, for understanding the civilian environment. So, any analysis of civilian environment and the way it is targeted or the way that resilience can be built needs to include at a minimum a gender analysis. To go further, and as we have already discussed, civilians as a group are divided not only by differences of gender, but also of race, nationality, ethnicity, religion, class, and sexual orientation. All of these differences both in self-identification and imposed categorisation have an impact on the position and power of individuals and the ways in which they may be actors both in creating hybrid threats, and in reacting to them and resisting them.

However, whilst civilians consists of and includes all genders, gendered constructions of civilian society have traditionally reduced civilians to be gendered as "female". The gendered approach to civilians during warfare, where women are seen as "innocent", "inactive" and "to be protected" has been projected onto the notion of "civilian" as a whole so that a gendered opposition is built between (simplistically) men and women. Within this dichotomy, men are actors of warfare who should protect the "vulnerable" women and children in the civilian population. Whilst hybrid threats are different from "classic" warfare, and threaten civilian populations in numerous and diffuse ways, this gendered dichotomy persists. This problematizes the extent to which we can examine "civilians" as actors in crisis and war and points to the need to deconstruct dominant understandings and representations of "civilians", and to analyse more closely the hierarchies and differences within civilian populations.

This is relevant when looking at men and women as actors of hybrid warfare. How do these men and women engage in hybrid warfare and pose hybrid threats? One of the tools of hybrid threat is that of dis-/mis-information, often spread through social media. Gender is important in understanding both the originators and the receivers of disinformation. It is well known that social media feeds and internet search results are constructed to show users results that cohere with what they already believe (for example by creating user profiles based on what a person has "liked" on their Facebook account). The resulting "filter bubbles" or "echo chambers" mean that users receive information and news consistent with their existing beliefs and preferences, and fake news can thus match these beliefs and preferences. Further, these algorithms are exploited by companies such as Cambridge Analytica which create profiles based on people's gender, sexual orientation, personality traits among others. Women and men can thus be targeted with different fake news stories which are more likely to resonate with their gender identity. These processes will additionally target other identity markers when and where relevant, often simultaneously.

3.3. Exploiting Gendered Social Cleavages

Recent and highly polarized debates over social issues such as violence against women, immigration and integration of migrant communities, the place of re-

ligion or secularism in European societies have provided fertile ground for the deployment of hybrid forms of threat which have sought to exacerbate and widen divisions based around these issues in society, and thus exploit vulnerabilities. As we noted earlier, disinformation does not always have to be hidden or always impossible to attribute. In fact, well-known websites or media sources can easily play a role in spreading disinformation, or at least, information that promotes polarized points of view and discord (towards destabilization) in a society (La Cour, 2020). Some Russian and pro-Russian social media sites and information sources have portrayed Western Europe and "European values" as a threat to their own "traditional" gender norms and regimes, through, for example the promotion of homosexuality and the breakup of the "traditional" family. As such in Ukraine, Russian soft power initiatives appealed to conservative values and opinions regarding family life and sexuality to try and convince Ukrainians of the dangers of Europe and its promotion of "sexual deviance" and the abolition of traditional gender norms and roles: "Not by chance, Russian media tried to compromise the recent mass protests in Ukraine, which started under pro-European slogans, by reducing European values to the issue of sexual minorities. In Russian social media Ukraine's pro-European choice has been often discussed in sexual terms, as a sexual deviation and an abandonment of gender norms' (Zhurzhenko, 2014: 259).

Within the EU, pro-Russian and anti-immigration social media sites have exploited long-standing disputes such as that over Muslim wearing the hijab in public spaces. The banning of hijab in public space or public employment in several European states has already led to public division, and this issue is thus one which has lent itself to manipulation. In highly gendered messages, Muslim women who wear a hijab are often depicted as oppressed or backward – victims of patriarchal cultures -, and at the same time as pawns used to encourage the Islamization of European society. In France, for example, where this debate has been ongoing for decades, following the passing of legislation to ban the wearing of hijab in public schools in 2004, the theme is one which is recurrent in far-right and anti-immigrant messaging. Recently this issue has recurred frequently in public debate and has been exploited by far-right and anti-immigrant movements through various social media channels (Bila 2019; Froio 2019; Schmelk 2017). In 2016 a significant online polemic was created following the decision of the mayor of Cannes to ban women from wearing a "burki-

ni" on the city's beaches, that was quickly overturned by the French Conseil d'Etat. However, this small legal quarrel was turned into a large-scale public debate through the online activity of a few far-right websites and social media accounts. In 2019 when the French sportswear store, Decathlon, decided to start selling hijabs adapted for running, another huge social media storm broke out accusing the store of wanting to "Islamize" France (Kaminski 2019).

The issue of the hijab is one which provides easy fuel for the far-right to provoke huge public reactions and stoke divisions. As well as protesting against the "Islamization" of France, they use arguments related to the defence of women's rights to protest against the hijab, and thus aim to enrol sectors of the public that would not necessarily be favourable to more classic far-right arguments. The normalisation of white supremacist theories and opinions in many countries, for example, can be explained by the ways in which some people are attracted to ideas which attribute superiority to their racial, gendered or ethnic category over "others".

The use of these types of arguments to create social divisions has been magnified with the so-called "refugee crisis" in Europe since 2015. The arrival of relatively large numbers of refugees, many from Muslim majority countries such as Syria, has proved to be a contentious issue for many European countries, and the use of the language of "crisis" by politicians and the media has contributed to making this an issue which can be used by actors wishing to create or exacerbate social divisions within EU societies. The securitization of migration has been built around representations of migrants as a threat to Europe, and in particular as responsible for violence and crime, and the issue of migration has been seized as an opportunity for those wishing to disrupt European unity and undermine European citizen's confidence in political leaders and institutions (Juhasz and Szicherle, 2017). These threats have often focused on gendered issues, but also simultaneously race and ethnicity, and have employed particular representations and stereotypes of men and women to gain momentum. The threat of "Muslim" or "migrant" men to "European" women has, for example, become a key theme in this type of influencing. Migrant men are frequently depicted as predatory and sexually aggressive, posing a particular threat to European women. It is argued that the countries and cultures from which they come do not respect women's rights, and have very low levels

of gender equality, and thus the men from these countries do not understand "European values" of gender equality or respect for women's rights. Thus, for example, Sweden has been labelled the "rape capital" of Europe by websites which link the high per capita number of refugees in the country to an alleged high risk of rape for Swedish women (BBC 2017). A series of websites linked to Russia and Hungary have published stories citing statistics from the Swedish National Crime Prevention Council to support their claims of massive increases in rape and sexual assault which these sites link to the large number of refugees in Sweden. However, the statistics are used out of context, failing to note the ways in which legal amendments in the definition of sexual assault and changes in methods for recording these in public data are in fact responsible for the changing figures on these crimes (Juhasz and Szicherle, 2017).

The widespread reporting of the sexual assaults supposedly carried out by "migrant" men in Cologne on New Year's Eve 2015 is a well-known example of the way in which this threat by male migrants to European women has been perpetuated. When some women reported that they had been sexually assaulted during the New Year's Eve celebrations in the city, there were quickly widespread media and social media reports claiming that these attacks had been coordinated by migrant and refugee men, although there was no accurate proof or reporting of this. The Cologne case sparked further reports of other similar attacks. Bild newspaper was forced to apologise in February 2017 after it published a report that a "mob" of migrant men had assaulted women in Frankfurt (Eddy 2017). In a report published on 6 February 2017, Bild, "quoted Jan Mai, the owner of a cafe in Frankfurt, as saying that 50 "Arab-looking men" had assaulted women on 31 December 2016. It also quoted a woman it identified only as Irina A., 27, who said she had been among those who were groped "everywhere" by the men" (ibid). However, the police affirmed that there was no evidence that this crime had taken place, and the newspaper was forced to apologise for publishing a false story. In 2016, the "Lisa" case swept to the forefront of German news. Russian TV and media reported widely on the case of a thirteen-year-old Russian-German girl who had gone missing in Germany, and who had supposedly been kidnapped, beaten and raped by three migrants of Arab origin (McGuinness 2016). The information was quickly spread through social media and the internet and led to the organisation of demonstrations by extreme-Right groups

in Germany (Sablina 2019). The claims that Lisa had been kidnapped were quickly shown to be false – she had been staying with a friend – but the rumours and false information persisted. The German police, Lisa and her family themselves publicly denied the story, but the Russian backed media that had featured the report did not issue an apology. They continued to frame the story as showing that Germany had a problem with policing and controlling migrants who were carrying out acts of sexual violence against women and girls (Baade, 2018). Even in 2018, Russian media sources continued to propagate the idea that the "Lisa case" was not fake because German courts have not imposed any punishment on Russian media sources for diffusing false information (Jakub, 2016).

The use of gendered representations of migrant threats to create social divisions, also has implications for the ways that white men are represented as being under threat from feminists, migrants, and all those who are supporting gender equality or migrant rights. The use of traditional gender roles is a major factor in the way that men and women belonging to alt-right movements choose to portray themselves on social media and to try and exert influence on others. The alt-right has been described as containing unifying themes which prioritise a fear of difference, whether that difference be sexual, gendered, religious, or racial. A cult of masculinity manifests itself in an "obsession with sexual politics and the heteronormative gender roles embodied in the nuclear family" (Marwick and Lewis, 2017: 12).

Membership of alt-right groups is predominantly male. Bergman (2018) conducted an comprehensive analysis of rank-and-file supporters of the Alt-Right and argues that the movement promotes a sense of "male entitlement" which, in turn, is "easily radicalized and connected to white nationalism and white supremacy" (Bergman, 2018 in Fielitz and Thurston 2019: 34). By attacking feminism and liberal notions of gender equality, the Alt-Right has "created a culture of vitriolic defensiveness among young white males, which aims to establish a common belief in white male victimhood" (ibid). The Alt-Right's existence, in part, relies upon a rejection of the accomplishments of feminism (ibid; May and Feldman, 2019). These messages are spread through social media sites and target white men in order to radicalise them and create resistance to government and existing social structures, ultimately resulting in acts of violence and conflict within societies: "Far-right

movements exploit young men's rebellion and dislike of , 'political correctness', to spread white supremacist thought, Islamophobia, and misogyny through irony and knowledge of internet culture. This is a form of radicalization happening primarily through forums, message boards, and social media targeting young men immersed in internet culture" (Marwick and Lewis, 2017: 29).

Images of women (perceived as conventionally attractive/beautiful) have been stolen and used on fake social media accounts to target and attract men to these accounts. In particular, images of "attractive" white women have been stolen and employed by Russian backed social media bots to attract white heterosexual men. For example, a former beauty queen, Rachel Hunter, was targeted in this way, when her image was stolen and used to front an alt-right facebook account in order to attract men to the movement. One study on the activity of troll social networks linked to the war in Syria, revealed that when experts published reports or articles that were critical of Russia or of the Bashar El Assad regime, they were instantly trolled by hundreds of fake accounts,"presenting themselves as attractive young women eager to talk politics with Americans, including some working in the national security sector" (Weisburd, Watts and Berger, 2016). These accounts which present themselves as belonging to attractive women are termed "honeypot" accounts, aimed to lure men into following and engaging with them.

There are some women in the Alt-right movements and they also reject "feminism" and adhere to ideas promoting women's "complementary" role to that of men, as housewives and mothers, reproducing "white" families (Mattheis, 2018). Images and representations of "traditional" male roles and hypermasculinity have also been used in Russia's information warfare campaign in Ukraine. Research has shown the way in which hypermasculine images of Putin have been used to emphasize the strength of Russia, whilst Ukrainian leaders and their Western European supporters were targeted as feminised or homosexual to show their weakness and supposed decadence (Romanets, 2017). One report on a Russian "troll factory" pushing out social media posts to undermine Russian opponents described a bank of humiliating images of Western leaders, including one of the then Ukrainian president Poroshenko in drag declaring "We are preparing for European integration" (Walker, 2015).

4. Conclusion

Looking at the ways in which men and women may engage in hybrid warfare differently, and may be targeted in varying ways, also allows us to think about different levels and strategies of resilience and resistance which might be employed by men and women, amongst different dominant or marginalized identity groups. Researchers have previously made the argument that more gender equal societies may be more peaceful and less likely to engage in war. We could also suppose that societies which were more gender equal might be more resilient to the type of hybrid warfare which involves weaponizing social divisions such as those discussed above to create civil conflict. If, as we have argued above, hybrid threats such as fake news or disinformation, and misinformation, seek to use existing inequalities and faultlines in societies and to weaponize these to create increasing social conflict, it stands to reason that societies which are more equal, have fewer disparities based on gender, race, class, ethnicity, nationality etc, and have more solidarity between citizens, are harder to destabilise in this way, and thus more resilient. Udupa and Pohjonen (2019) propose an "extreme speech" framework which emphasizes ethnographic sensibilities of certain cultural contexts which make them more receptive to certain types of hate speech and disinformation. This framework focuses on systematic enquiries into histories of racial construction and hierarchies which can be weaponized to provoke social conflict. We suggest that the addition of a focus on constructions of gender norms and hierarchies could be added to provide an intersectional framework to understand the ways in which social resilience to disinformation can be reinforced.

Using intersectional approaches to analysis allow us to understand broader, complex regions that are increasingly targeted by hybrid threats. But more needs doing. Some research is being accumulated with regard to democracies in the global north but less is being done with a view to the global south, where more newly emerging democracies can be extremely vulnerable to possible influence operations, misinformation and disinformation. There is a gap in literature exploring various angles of hybrid threats and warfare in the global south, especially in Africa. The existing literature on African cases explores very little to what extent technologies affect institutions, crises management or norms (and vice-versa).

Most of the scholarship revolves around social media and elections (Ndlela & Mano, 2020), digital dictatorship and democracy (Gopaldas, 2019), separatism, hate speech (Ibrahim et al, 2019) and its social impacts (Aganze & Kuslinga, 2020). Despite this lack of theorization, some studies are starting to emerge such as the attempt to understand for example motivations for sharing mis-/disinformation by comparing African countries (Wasserman et al, 2019). Such research is imperative both to understand impacts of hybrid attacks on emerging democracies, but also for comparative benefits. Democracies in the global south may be "emerging", but so is power from this region, with an increasingly well-connected and technology savvy, young population. In the case of the global south, for example, there is no research exploring the implications of postcolonialism (including gendered norms) in hybrid warfare/ threats. As such, gender and intersectional analyses of hybrid threat scenarios open up the doors to a better understanding about how hybrid threats function, across contexts, making use of identity markers from gender to race and ethnicity, from age to class or sexual orientation. The literature (on security, disinformation, hybrid warfare etc.) has not yet addressed the implications of the management of those crises and the dynamics of trust, security and resilience at play. The roles structures of domination, oppression, inequality etc. play in hybrid threat processes can no longer be ignored.

References

Aganze, E., & Kusinza, R. (2020). The Current State of Fake News in the DR Congo and Socials Impacts. *Global Journal of Computer Science and Technology*.

Ake, Claude. 1975. "A Definition of Political Stability." Comparative Politics 7 (2): 271–83.

Baade, B. (2018). "Fake News and International Law". *European Journal of International Law, 29*(4), 1357-1376

Baines E and Paddon E (2012) 'This is how we survived': Civilian agency and humanitarian protection. *Security Dialogue 43*(3): 231–247.

Bajarūnas, E. (2020). Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond. *European View*, 1781685820912041.

Bartkowski, M. (2015). Nonviolent civilian defense to counter Russian hybrid warfare. *John Hopkins University*. Oţujak.

Batyuk, V. I. (2017). The US concept and practice of hybrid warfare. *Strategic Analysis, 41*(5), 464-477.

BBC News (2017). "Reality Check: Is Malmo the 'rape capital' of Europe?" BBC News: Politics. 24 february 2017. Accessible at: https://www.bbc.com/news/uk-politics-39056786

Beccaro, A. (2018). Modern irregular warfare: The ISIS case study. *Small Wars & Insurgencies, 29*(2), 207-228.

Bergman, H. (2018): "White Men's Fear of Women: Anti-Feminism and the Rise of the Alt-Right". *The Examined Life Lab*, 31 March 2018.

Brânda, O. E., & Sauliuc, A. L. (2020, June). Hybrid Threats on NATO's Eastern Flank-A Comparative Analysis. In *International conference Knowledge-Based Organization* (Vol. 26, No. 1, pp. 33-41). Sciendo.

Bila, A. (2019). "Countering Islamophobia in France". In *Countering Islamophobia in Europe* (pp. 213-251). Palgrave Macmillan, Cham.

Bilgic, Ali; Hoogensen Gjørv, G and C. Wilcock. (2019). "Trust and Distrust in the Politics of Security: An Untrustworthy Immigrant in a Trusting Nordic Community" *Journal of Political Psychology*. *40*(6): 1283-1296.

Burgers, T., & Romaniuk, S. (2016). Hybrid Warfare in the South China Sea: The United States' Little Grey (Un) Men. *The Diplomat*.

Carastathis, A. (2014), 'The Concept of Intersectionality in Feminist Theory.' *Philosophy Compass, 9*(5), 304-14.

Carden, James (2017) "Russia and America's Dangerous Dance," The National Interest. Retrieved 6 December 2020. Available: http://nationalinterest.org/feature/russia-americas-dangerous-dance-11798

Dunn Cavelty, M., Kaufmann, M., & Søby Kristensen, K. (2015). Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue, 46*(1), 3–14. https://doi.org/10.1177/0967010614559637

Chandler, D. (2012). "Resilience and human security: The post-interventionist paradigm." *Security Dialogue 43*(3): 213-229

Chandler, D. (2014). "Beyond neoliberalism: resilience, the new art of governing complexity." Resilience: International Policies, *Practices and Discourses 2*(1): 47-63. Clark-Kazak 2014

Choo, K.-K. R. (2011). "The cyber threat landscape: Challenges and future research directions." *Computers & Security 30*(8): 719-731.

Coaston, Jane. 2019. "*The Intersectionality Wars*." Vox, 2019.

Cohen, O., A. Goldberg, M. Lahad and L. Ahronson-Daniel (2016). "Building resilience: The relationship between information provided by municipal authorities during emergency situations and community resilience." *Technological Forecasting & Social Change* 121: 119-125

Considine, L. (2015). "'Back to Rough Ground!' A Grammatical Approach to Trust and International Relations." Millennium - *Journal of International Studies 44*(1): 109-127.

Crenshaw, K. (1991). Mapping the margins: Intersectionality, identity politics, and violence against women of color. *Stan. L. Rev., 43*, 1241.

Cullen, P. J., & Reichborn-Kjennerud, E. (2017). MCDC countering hybrid warfare project: Understanding hybrid warfare. *A Multinational Capability Development Campaign project*, *London*.

Derakhshan, H., & Wardle, C. (2017). Information disorder: definitions. A*A. VV., Understanding and addressing the disinformation ecosystem*, 5-12.

Eddy, Melissa (2017). "Bild Apologizes for False Article on Sexual Assaults in Frankfurt by Migrants." *The New York Times*. 16 february 2017. Accessible at: https://www.nytimes.com/2017/02/16/world/europe/bild-fake-story.html

Egelhofer, J. L. and S. Lecheler (2019). "Fake news as a two-dimensional phenomenon: a framework and research agenda." Annals of the International Communication Association 43(2): 97-116.

EuropeAid (2016). "Building Resilience: The *EU's approach." EU FACTSHEET: Humanitarian Aid and Civil Protection Development and Cooperation*.

European Commission (2017). *Joint Communication to the European Parliament and the Council: A Strategic Approach to Resilience in the EU's external action*. High Representative of the Union for Foreign Affairs and Security Policy: European Union.

Fallis, D. (2014). *The Varieties of Disinformation*. *The Philosophy of Information Quality*. L. Floridi and P. Illari. New York, Springer.

Fearon, James D. 1994. "Domestic Political Audiences and the Escalation of International Disputes." *The American Political Science Review 88*(3): 577–92.

Fielitz, Maik and Nik Thurston (eds). Post-Digital Cultures of the Far Right: Online Actions and Offline Consequences in Europe and the US. Transcript Verlag, Beilefeld

Filipec, O. (2019). Hybrid Warfare: Between Realism, Liberalism and Constructivism1. *Central European Journal of Politics, 5*(2), 52-70.

Flore, M., A. Balahur, A. Podavini and M. Verile (2019). Understanding Citizen's Vulnerabilities to Disinformation and Data-Driven Propaganda. JRC Technical Reports. Luxembourg: Publications Office of the European Union, European Union.

Froio, C. (2019). Nosotros y los otros: la alteridad en los sitios web de la extrema derecha en Francia. *DeSignis*, (31), 241-270.

Fox, A. C., & Rossow, A. J. (2017). *Making Sense of Russian Hybrid Warfare: A Brief Assessment of the Russo-Ukrainian War*. Institute of Land Warfare, Association of the United States Army.

Gelfert, A. 2018. "Fake News: A Definition." *Informal Logic 38*(1): 84–117.

Ghaffari, H (2019). "The necessity of 'effective reaction' against U.S. hybrid war" Tehran Times. Retrieved 6 December 2020. Available: https://www.tehrantimes.com/news/437255/The-necessity-of-effective-reaction-against-U-S-hybrid-war.

Giannopoulos, G, H Smith, and M Theocharidou. 2020. *The Landscape of Hybrid Threats : A Conceptual Model*. European Commission, Ispra. JRC117280.

Giegerich, B. (2016). Hybrid Warfare and the Changing Character of Conflict. *Connections, 15*(2), 65-72.

Gopaldas, R. (2019). Digital Dictatorship versus Digital Democracy in Africa.

Haynie, J. (2020). *Putin's Hybrid Wars: A Comparative Analysis of Russian Incursions into Georgia, Ukraine, Bulgaria, and Syria* (Doctoral dissertation, Kent State University).

Heffington, Colton. 2017. "Marked Targets: Coercive Diplomacy and Domestic Terrorism." *Journal of Global Security Studies 2*(2): 123–36.

Herrero-diz, P,Pérez-escolar M, and Juan F Plaza Sánchez. 2020. "Gender Disinformation : Analysing Hoaxes on Maldito Feminismo." *Icono 14 18*(2): 188–215. https://doi.org/10.7195/ri14.v18i2.1509.

Hoffman, Frank G. 2007. "*Conflict in the 21st Century: The Rise of Hybrid Wars*." Arlington, VA.

Hoffman, Frank G. 2018. "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges." *Prism 7*(4): 30–47.

Hoogensen, G. and Stuvøy, K. 2006. Gender, Human Security and Resistance. *Security Dialogue 37*(2): 207-228.

Hoogensen Gjørv, G. 2017. "Human Security" in *Security Studies: An Introduction*. Paul Williams and Matt MacDonald (eds). London: Routledge.

Hoogensen Gjørv, G. 2020. "Coronavirus, invisible threats and preparing for resilience" *NATO Review*. Available at: https://www.nato.int/docu/review/articles/2020/05/20/coronavirus-invisible-threats-and-preparing-for-resilience/index.html?fbclid=IwAR3s3TTYuY3CdigsdS8me1vSh5lKCHSlqkQKLonSdprcIPuZkU-2aWwVTqA

Hoogensen Gjørv, G. and Ali Bilgic (forthcoming 2021) *Positive Security*. London: Routledge.

Horton, A. (2020). "After Truth: how ordinary people are 'radicalised' by fake news." The Guardian Retrieved 18 May 2020, from https://www.theguardian.com/tv-and-radio/2020/mar/19/after-truth-hbo-fake-news-pizzagate-documentary https://mathias-nilges.com/student-projects-the-new-culture-wars/2018/4/1/white-mens-fear-of-women-anti-feminism-and-the-rise-of-the-Alt-Right

Ibrahim, A. M., Adamu, M. A., & Lawan, A. K. Fake News of Fat Nuisance? Theorising Fale News in a Nigerian Context in relation to Democratic Process. *Asian Journal of Applied Communication e-ISSN, 2682*, 7506.

Jakub, J. (2016). *The Lisa Case: STRATCOM Lessons for European states* (No. 11). Security Policy Working Paper.

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.

Juhász, A., and Szicherle, P. (2017). The political effects of migration-related fake news, disinformation and conspiracy theories in Europe. *Friedrich Ebert Stiftung, Political Capital, Budapest*.

Kaminski, D. (2019). « Hijab de course et running à l'échalote ». *La Revue Nouvelle*, (3), 24-25

la Cour, C. (2020). « Theorising digital disinformation in international relations ». *International Politics*, 1-20.

Lanoszka, A. (2016). "Russian hybrid warfare and extended deterrence in eastern Europe." *International Affairs 92*(1): 175-195.

Lindley-French, J (2015). *NATO: Countering Strategic Maskirovka*. Calgary: Canadian Defence and Foreign Affairs Institute.

Mac Ginty R (2010). Hybrid peace: The interaction between top-down and bottom-up peace. *Security Dialogue 41*(4): 391–412. DOI: 10.1177/0967010610374312.

Major, C. and C. Mölling (2015). "A Hybrid Security Policy for Europe: Resilience, Deterrence, and Defence as Leitmotifs." Stiftung Wissenschaft und Politik 22(April 2015): 1-4.

Marwick, A., and Lewis, R. (2017). Media manipulation and disinformation online. *New York: Data & Society Research Institute*.

Mattheis, A. Shieldmaidens of Whiteness:(Alt) Maternalism and Women Recruiting for the Far/Alt-Right. *Journal for Deradicalization*, (17), 128-162.

May, R., and Feldman, M. (2019). Understanding the Alt-Right: Ideologues, 'Lulz' and Hiding in Plain Sight. In Fielitz, Maik and Nik Thurston (eds). Post-Digital Cultures of the Far Right: Online Actions and Offline Consequences in Europe and the US. Transcript Verlag, Beilefeld: 25-26.

McGuinness, D (2016). "Russia steps into Berlin 'rape' storm claiming German cover-up" *BBC News: Inside Europe* Blog. 27 January 2016. Accessible at: https://www.bbc.com/news/blogs-eu-35413134

Meerow, S., J. P. Newell and M. Stults (2016). "Defining urban resilience: A review." Landscape and Urban Planning 147(March): 38-49.

Meister, S. (2016). "The "Lisa case": Germany as a target of Russian disinformation", *Nato Review*, 25 July 2016.

Mohanty, Satya P. 2018. "Social Justice and Culture: On Identity, Intersectionality, and Epistemic Privilege." In Handbook on Global Social Justice, edited by Gary Craig, 418–27. Cheltenham, UK: Edward Elgar Publishing Inc.

Mumford, A. (2016). The Role of Counter Terrorism in Hybrid Warfare. *CEO-DAT, November*.

Muradov, I. (2019). *The donbas conflict as a form of Hybrid Warfare: A Neoclassical Realist Analysis* (Doctoral dissertation, Middle East Technical University).

NATO (2020). "Resilience and Article 3" Topics. Accessible at: https://www.nato.int/cps/en/natohq/topics_132722.htm?selectedLocale=uk

Ndlela, M. N. (2020). Social Media Algorithms, Bots and Elections in Africa. In *Social Media and Elections in Africa, Volume 1* (pp. 13-37). Palgrave Macmillan, Cham. O'Loughlin 2015

Raska, M. (2015). "Hybrid Warfare with Chinese Characteristics". *RSIS Commentary. No.262. S. Rajaratnam School of International Studies*, Nanyang Techological University.

Raţiu, A., & Munteanu, A. (2018). Hybrid warfare and the Russian Federation informational strategy to influence civilian population in Ukraine. *Land forces academy review, 23*(3), 192-200.

Reichborn-Kjennerud, E, and P Cullen. 2016. "*What Is Hybrid Warfare ?"* Policy Brief, no. 1. Norwegian Institute of International Affairs (NUPI).

Romanets, M. (2017). Virtual warfare: Masculinity, sexuality, and propaganda in the Russo-Ukrainian war. *East/West: Journal of Ukrainian Studies, 4*(1), 159-177.

Roloff, R., & Dunay, P. (2018). The Age of Post-Truth: State Influence and Strategic Communication–Contemporary Security Challenges on Europe's Eastern Flank. *Connections: The Quarterly Journal, 17*(2), 19-38.

Sablina, L. (2019). "We Should Stop the Islamisation of Europe!": Islamophobia and Right-Wing Radicalism of the Russian-Speaking Internet Users in Germany. *Nationalities Papers*, 1-14. doi:10.1017/nps.2019.76

Sahin, K. (2017). "Germany Confronts Russian Hybrid Warfare." Retrieved 18 May 2020, from https://carnegieeurope.eu/2017/07/26/germany-confronts-russian-hybrid-warfare-pub-72636

Schmelk; C. (2017). « Plongée en fachosphère ». *Médium*, 52-53(3-4), 199-212. https://doi.org/10.3917/mediu.052.0199

Shu, K., Mahudeswaran, D., Wang, S., Lee, D., & Liu, H. (2020). FakeNewsNet: A Data Repository with News Content, Social Context, and Spatiotemporal Information for Studying Fake News on Social Media. *Big Data, 8*(3), 171-188.

Sørensen, Heine and Nyemann, Dorthe Bach (2018). "Going Beyond Resilience: A revitalised approach to countering hybrid threats." *Strategic Analysis* November 2018. Helsinki: Hybrid CoE.

Tierney, K. J. (2015). "Resilience and the neoliberal project: discourses, critiques, practices - And Katrina." *American Behavioural Scientist 59*(10): 1327-1342.

Udupa, S. and Pohjonen, M (2019). "Introduction: Extreme Speech and Global Digital Media Cultures",*International Journal of Communication 13*: 3019–3067. Veebel, 2020

Walker, Shaun. "'Salutin' Putin: Inside a Russian Troll House." The Guardian, 2 Apr. 2015, https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house?C

Watts, T., & Biegon, R. Conceptualising Remote Warfare: The Past, Present, and Future. *Oxford Research Group*.

Weisburd, A., Watts, C. and Berger, J. (2016), "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy," War on the Rocks, November 6, 2016, https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy

Wither, James K. 2016. "Partnership for Peace Consortium of Defense Academies and Security Studies Institutes Making Sense of Hybrid Warfare." *Connections 15*(2): 73–87.

Yuval-Davis, N. (2011), *Intersectionality and Feminist Politics*, London: Sage Publications.

Zaliznyak, Y. (2016). Information security and Russian aggression: Ukraine–EU–NATO hybrid response to hybrid war. *Rocznik Instytutu Europy Środkowo-Wschodniej, 14*(2), 23-42.

Zhurzhenko, T. (2014). A divided nation? Reconsidering the role of identity politics in the Ukraine crisis. *Die Friedens-Warte*, 249-267.

Notes

[1] https://ethicaljournalismnetwork.org/tag/fake-news/page/2

[2] https://ethicaljournalismnetwork.org/tag/fake-news/page/2