# AFF

### AT: Hybrid War K---2AC

#### Researching the methods and culture of hybrid war is important---rejecting “hybrid war” exacerbates the danger it poses.

Andriy Tyushka 19, Senior Research Fellow in the European Neighbourhood Policy Chair, 2019, “Hybrid War(fare): The Challenge of Contagion,” 2019, Torun International Studies, Issue 12, pp. 5–29, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-c63913a7-9115-4d4a-8c3e-a620eeb5d495

With great (power) wars past long ago and today’s decline of inter-state conflicts worldwide, with Pax Americana and Pax Europaea largely enduring since the end of the WWII (thus, democratizing nations and relations among them)1 , a Fukuyama-styled decisive victory of a liberal democratic order willy-nilly crosses one’s mind. And yet, the 1989-declared ‘end of the history’ has to be postponed – again:

‘There is a feeling abroad today that Western civilization is on trial before history. One of the clearest signs of it is the increasing frequency with which we hear the word “challenge” in connection with the policies and progress of Soviet [Putin’s] Russia and the Communist [illiberal] world at large’ (Tucker 1959: 1) (edits to the original mine. – AT).

It sufficed two tiny edits (updates – if you wish) in the afore-quoted statement to render the strategic world-political assessment of the 1960s-peaking Cold War, made by a renowned American Sovietologist at Harvard and Princeton Universities, its full-sound quality and resonance in the realities of our-age and twenty-second century global politics

Indeed, just a decade ago, as Russia’s military campaign in Georgia was unfolding, the near and far neighbourhood’s discourses were intensively echoing questions such as: ‘Is Ukraine next?’ Some half a decade ago, as Russia’s less conventional military aggression and political subversion campaign in Ukraine erupted, questions did resonate in the region and far beyond: ‘Are the Baltic states of Latvia, Lithuania and Estonia next’2 ? Couple of years ago, as Russia’s covert military and political overtures in Syria and Libya, US and the UK, Germany, France, Poland, the Netherlands and so forth unraveled, the answers to the question ‘who’s next?’ seem to have been tacitly found – at least no more geographical directions are being pointed to. The paradox discovered here lies in the simplicity that was self-delusively denied being accepted in many European capitals: the genuine realist answer to the ‘what/where/ who next?’ question has always been ‘where necessary – to defend national interests’ (however defined). Waging a hybrid war(fare) has become one of the proven ways to defend Russia’s interests in near and far neighbourhoods. Rather disturbingly, it is incrementally becoming a preferred way to advance interests of other state and non-state actors. The spread of the hybrid warfare methods and the culture of hybrid war as such is a new reality to which the policymakers and scholarly communities alike need to wake up.

A number of analytical works written so far have been dedicated to disentangling the hybrid warfare’s nature and manifestations, i.e. the art of war. It is of little use if it is not accompanied with the analysis of ‘whose war?’ problem in the sense of seeking response to the fundamental questions who is waging the war (aggressor), to what end (broad strategic and tactical aims), against whom (war targets and theatres) and who will stand in defence (national and/or collective defence and deterrence)? The vast majority of these questions is left unanswered in much of the scholarly and policy writings. Ambiguity and deliberate straight-talk avoidance abound. Ambiguity is the best bedfellow of hybrid war(fare). Thus, as long as there is a lack/avoidance of clarity in scholarly and political answers to the aforementioned questions, the international constellations will remain thriving for a spatial and temporal contagion of hybrid war(fare).

This article seeks to problematize the contagion of hybrid war and hybrid warfare – both with the zoom on Russia and in a much wider world-political perspective: geographic, temporal and agential.

With no pretense to pathetic or inflated claims, this article casts a broad analytical perspective on the creeping hybridization of war and order and posits that the phenomenon is there to stay unless strategically contained and devaluated as a proliferating means of twenty-first century politics. Thereby, it invites thinking beyond ‘the Ukraine crisis’ and ‘the Russia challenge’ in (Eastern) Europe – i.e. a well-founded, though, admittedly, a way too narrow (both spatially and temporally, as well as in terms of agency and warfare modalities) hyper-focus in much of the political and academic debate today. The currently observed expansion of Russia’s theatres of hybrid war(fare) from Ukraine to Middle East, Europe and the US, as well as the tactical variance and constant innovation of warfighting methods, as practiced and mutually observed/emulated by agents beyond Russia (such as Iran, China, or the ISIS), points to the pertinence of broader emerging trends that concern the foundations of international theory, strategic and military studies – rather than policy or area studies alone. The contagion effects of hybrid war(fare) discursive and political practices across the globe is what shapes the core analytical puzzle of the current article. Focusing on the ontologies of the hybrid war and warfare contagion, as evidenced in proliferating ideologies and politics of hybrid war(fare) as well as richly documented in policy analyses and scholarly literature, this article problematizes the agency (action-reaction) dilemmas for both states and societies directly targeted by such hostile campaigns as well as the international (liberal democratic) community at large.

#### Perm---do both---the AFF renegotiates the scope of A5 in light of an armed attack which solves the K.

Maria Mälksoo 18, Senior Lecturer in International Security at the Brussels School of International Studies at the University of Kent, 2018, “Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO,” European Security, Vol. 27, Issue 3, pp. 374-392, <https://www.tandfonline.com/doi/full/10.1080/09662839.2018.1497984>

NATO

“Hybrid warfare” has emerged as yet another “resilience test” (Stoltenberg 2015a) for the Alliance in its post-Cold War existential search for a new purpose and mission. Moreover, the hybrid insecurity predicament enables the allies to bring together the renewed focus on NATO’s traditional mission (i.e. endorsing collective defence in order to counter the main geopolitical contestant of the North Atlantic Alliance in Europe) and the Alliance’s post-Cold War out-of-area military expeditions. While “tak[ing] on two different forms of strategic challenges simultaneously” – that is, “the Russian hybrid warfare approach” and that of “other non-state actors like ISIS to the south” – remains NATO’s “greatest challenge”, the common idea behind these “hybrid strategies” endorses the relevance of “a comprehensive approach across the DIMEFIL spectrum” (i.e. diplomatic/political, information, military, economic, financial, intelligence, legal) for NATO (Breedlove 2015, p. xxv; cf. Bell 2012, pp. 225–226). The “beauty of the hybrid warfare concept” is accordingly seen to lie in its ability to “provide tools for a comparative strategic perspective of NATO’s southern and eastern flanks, while allowing for a differentiated response” (Johnson 2015, p. 276). NATO’s motto in the face of these twofold challenges is called to be “adopt, adapt, adept”: the new strategies adopted to deal with the hybrid threats to NATO’s East and South need to be accompanied by NATO’s adaptation of “its structure and readiness to become adept at handling the new challenges it faces” (Calha 2015, p. 9).

Countering hybrid threats posed by Russia and the Islamic radicals threatening the territories, populations, interests, and values of the Alliance thus enables NATO to endorse its continuing relevance by constructing a strong narrative and maintaining its OS as the core security guarantor for its members (cf. Flockhart 2012, pp. 78–79). The softer, partnershipgeared, or so-called “Jane” narrative of the early-post Cold War NATO is clearly giving way to a more familiar, hard security-focused “Tarzan” self-vision and public representation (see further Flockhart 2011). Calling the kettle black is the least of NATO’s worries: Russia’s use of “proxy soldiers, unmarked Special Forces, intimidation and propaganda, all to lay a thick fog of confusion; to obscure its true purpose in Ukraine; and to attempt deniability” is explicitly dissected in outlining NATO’s emerging counter-strategy to hybrid engagements of the sort (Stoltenberg 2015a). Yet, just the traditional set of NATO’s capabilities is clearly deemed to be insufficient in the face of, inter alia, “sophisticated disinformation and radicalization campaigns” (Stoltenberg 2015b), this more forceful and traditional antagonist-driven agenda reflects NATO’s long-pursued comprehensive approach – that is, “a combination of military and non-military means to stabilize countries” (that others use to “destabilize”) (Stoltenberg 2015a). “Hybrid” is accordingly coined as “the dark reflection” of NATO’s comprehensive approach, and accordingly, early warning and situation awareness, good governance and the resilience of societies become equally essential parts of deterrence and defence against hybrid threats (Stoltenberg 2015a). This necessitates “renewed attention to strategic communications” and public outreach and education “to build up public awareness and resilience” and “strengthen the role of an informed civil society in every member state” (Calha 2015, p. 10).13

NATO declared its readiness to address the specific challenges posed by “hybrid warfare threats” in the Wales Summit Declaration of 5 September 2014 as a forceful response to the conflict in Ukraine. While NATO’s traditional toolbox of collective defence is hardly perfectly geared for “insidious and ambiguous threats” (Johnson 2015, p. 270, Calha 2015, p. 4), countering hybrid warfare emerges as a continuing relevance and resilience test for the Alliance. NATO’s institutional responses to “hybrid threats” have been further detailed in its Readiness Action Plan, a roadmap for building capability packages, a comprehensive concept for creating an enhanced NATO response force, in a classified strategy for hybrid warfare and a cyber security action plan. Altogether, the ambiguity and gradient nature of hybrid tactics directly challenge the ontological underpinnings of NATO’s core mission and strength as hybrid activities might “progress incrementally towards a threatening situation while remaining under NATO’s Article 5 threshold” (Calha 2015, p. 4). The detection and definition of a threat hence becomes significantly less straightforward, pointing at the need to renegotiate the scope and substance of NATO’s collective defence clause (i.e. Article 5 of the Washington Treaty) in light of the contemporary hybrid engagements.

### AT: Hybrid War K---Offense

#### Hybrid war is real and dangerous.

Andriy Tyushka 19, Senior Research Fellow in the European Neighbourhood Policy Chair, 2019, “Hybrid War(fare): The Challenge of Contagion,” 2019, Torun International Studies, Issue 12, pp. 5–29, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-c63913a7-9115-4d4a-8c3e-a620eeb5d495

Certainly, an unnecessary reverberation (if not simply a hype) of the term bears nasty consequences for policy response as the first question being naturally advanced is whether the hybrid warfare talk is ‘much ado about nothing’ or a serious concern about the emerging security gap? In a way, the entire problematique gets ridiculed to the somewhat simplified and overgeneralized dilemmatic question to be resolved: is it prudent or paranoid to talk about proliferating hybrid threats and hybrid world order? Rich empirical evidence, which is only selectively presented in the next section, suggests a positive answer to the afore-stated question.

3. EXPLORING HYBRID WARΈFAREΉ CONTAGION: TRENDS AND GEOGRAPHIES

Evidence from much of the public, political and academic debate convincingly demonstrates: the proliferation of hybrid war and warfare are more than a ‘buzzword’ matter – legible concerns about it incrementally grow across the nations, regions and even entire continents, with some being more and some less affected by hybrid war(fare) contagion. Both public, political and academic issue salience point to such a conclusion.

For instance, the hybrid war(fare) topic trending in public discourse exhibits quite a revealing picture of issue salience since at least 2004, with the European terrain being the epicenter of public attention to the issue in question (cf. Figure 2). The geographical spread of hybrid war(fare) – or a threat thereof, as perceived in public discourses, is most concentrated around the top topic-trending countries, with Ukraine – rather expectedly – enjoying the place of the most important locus of attention, followed by Poland, Estonia, Bulgaria and Georgia, Croatia, Czechia, Latvia, Belarus, and Finland on the top-10 list.

**[Omit Figure 2]**

In policy debate, the hybrid war(fare) topic salience can be observed in a number of world’s regions – from the topic-trending Russia and the former Soviet Union space to integrated Europe and North America, but also Middle East, Asia and Africa (cf. Table 1).

**[Omit Table 1]**

As seen from the table, hybrid warfare clearly presents a salient policy issue for Russia’s neighbours – first and foremost, Ukraine, Belarus, CEECs such as Poland or Czechia as well as the Baltic states. Within the so-called Commonwealth of Independent states (CIS) alone, the situation is quite telling as ‘[e]ach of Russia’s reform-minded neighbours is plagued by “separatism”4 [ – and] it’s no coincidence’ (Orttung and Walker 2015). Of course, the scope and extent of hybrid threats is bigger than that: in addition to the weaponization of self-determination (so-called astroturfed ‘separatism’), both information and culture, economics and democratic openness, etc., are seen being weaponized within respective hybrid warfare stratagems.

Finally, the evidence of hybrid war(fare) topic salience can also be found in the academic debate, as the herewith undertaken bibliometric analysis shows. Whereas the current article’s effort is concentrated on pinpointing the academic salience of the topic as covered in major Web of Science indexed journals (cf. Figure 3), it should be acknowledged that the topic is covered much broadly in non-WoS indexed peer-reviewed journals. Still, the academic production corpus of WoS indexed journals reveals the topical salience of hybrid war(fare) in scholarly enquiries on security and defence affairs in Ukraine, the US, Romania, UK, Poland, Russia, Czechia, Germany, Austria and Italy. A clear gap in topic coverage by academic literature, as revealed by the WoS corpus analysis, is rather surprising compared to other indexed outlets as well as public and political debates – much broader in their geographic and issue-matter foci, with a centre of analytical gravity that massively revolves around Russia’s agency in that very context (at the expense of a wider perspective?).

**[Omit Figure 3]**

Thence, with a varying intensity and focus laid on state and non-state agency as well as geographic theatres of hybrid warfare operation, the topic is clearly salient in both public, political and academic debates, and this salience is very much predicted to expand further – together with the proliferation of the hybrid war culture and hybrid warfare methods among countries and regions worldwide.

An exponential rise of the ‘hybrid warfare’ phenomenon owes its dynamics particularly to the number of military and politically subversive operations Russia has undertaken since early 2014 in Ukraine’s Crimea and eastern regions of Donbas. The phenomenon is much broader both in terms of geographical and agential spread worldwide, with some parts of Eurasia, Middle East and Asia Pacific looming large as the hotbeds of this proliferating type of warfare below (classical understanding of) war.

Internet search retrievals abound in references to academic and policy writings as well as journalist investigations on the matter.

Official communications delivered by government officials and high-ranking international fonctionnaires worldwide, too, contain increasing references to the proliferation of ‘hybrid threats’ and the necessity of developing a suitable policy response – both in national and intergovernmental contexts.

All that points to a rather new development where the prerogatively military term and the related vocabulary of ‘hybrid warfare’ lose their exclusivity as concepts applied by, and relevant for ‘military strategists only’, thus entering the everyday political and diplomatic vocabulary as well as public discourses.

Whether in Estonia, Czechia or Poland (Schultz 2017), Germany, France or the Netherlands, Russia’s hybrid warfare operational theatre steadily expands to new sovereign terrains of the Western liberal democracies.

Following Russia’s resonant and highly plausible meddling in the 2016 US presidential elections, in 2017, then-presidential candidate Emmanuel Macron successfully dodged similar hack-and-leak cyber-attacks and fake news reports widely attributable to the Kremlin. In late 2018, the French authorities faced a renewed challenge of Kremlin’s digital offensive – now from among 600 Twitter pro-Kremlin accounts that, under the top hashtag #giletsjaunes, i.e. ‘yellow vests’, intensively fuel outrage of street protesters. Possible involvement of the Kremlin in amplifying the ‘yellow vests’ protests in France (cf. e.g.: Blakely 2018; Matlack 2018) is now being investigated by the French authorities in spite of Russia’s ‘traditional’ implausible denials

In response to the Skripal poisoning earlier in 2018, yet another widely attributed to the Kremlin undercover operation in Europe and the UK in particular, British PM Theresa May bluntly put it that ‘[t]he Russian threat does not respect borders, and as such we are all at risk’ (quoted after: McTague, 2018). The threat looms even more so large if one considers the strategic rationale of Russia’s hybrid gambit – in fact, an undeclared war against the Western-dominated world order and the hegemony of the liberal democracy as such.

In this war, Ukraine is only one of the many targets and theatres, which expand in both the scope and depth of engagement – as far as the strategic and operational goals will require

The case of Russia’s ‘hybression’, i.e. hybrid aggression, in Ukraine is quite illustrative when it comes to the contagion effects of (strategic) hybrid warfare proliferation.

First, the Blitzanschluss of Crimea (the so-called ‘self-determination’ staged by the Russian special operation forces), then the (failed) attempts to extend hybrid incursion to Ukraine’s wider South-East (the so-called ‘Novorossia’ offensive), successful detachment of Ukraine’s eastern areas (the so-called ‘separatism’ in Donbas region), and, more recently, renewed attempts to twist the ‘Novorossia’ offensive, now undertaken as a naval offensive in the Kerch Strait of the Sea of Azov. Not only did the geography of Russia’s operational theatre expand in Ukraine – every next struggle, however narrow (MacFarquhar 2018), risks wider war

Fifth year on, the contagion of Russia’s hybrid warfare can now however be traced far beyond Ukraine’s borders. Already back in 2015, Zbigniew Brzeziński, a senior political scientist and former adviser to the US-American President Jimmy Carter, was not sparkling with optimism as the Russian war in Ukraine was concerned. In the wake of his March 2015 visit to Poland, he put his advice for the compatriots in a very succinct and unequivocal passage: ‘Ukraine is not the endpoint. We have to be ready to defend ourselves’ (Brzeziński 2015).

Time and again, Polish intelligence agency ABW and investigative journalists uncover Russia-linked subversive groups who – via disinformation campaigns or political subversion (astroturfing, false flag outrage) – seek to exacerbate tensions both within the Polish society and with Ukraine – to sow discord between Poland and Ukraine, thus directly or indirectly promoting the Kremlin’s interests (DW, 2018). The tension in Polish-Ukrainian relations may resonate well beyond the confines of this bilateralism, not least in the context of Poland’s role as a key supporter of pro-Western policy attitudes in Ukraine and pro-Ukrainian policy attitudes in the European Union, both of which run contra Kremlin’s illiberal script for the post-Soviet space.

Up north in the Baltics, the spread of Russian hybrid warfare became a serious political concern the very moment Russia annexed Crimea from Ukraine in early 2014. Whether the Baltic states were (to be) next, has been since then one of the permeating questions in security debate both within the small region and Europe-wide (Radin 2017).

A number of other European countries and Western democracies have been affected by the spread of Russia’s hybrid war from Crimea to Salisbury, for the past five years now. Whereas tracing (and predicting) the contagion effects of hybrid warfare in toto is quite a daunting task – not least because of the problematic means identification and agency attribution, its main components, such as information weaponization (fake news spread, public and media propaganda campaigns) or ‘weaponized self-determination’ (external orchestration, partisan sponsoring or otherwise supporting of ‘self-determination’ processes regionwide), can be feasibly analyzed. For instance, Cunningham and Sawyer’s (2017: 598) spatial analysis of the spread of self-determination claims – statistically – confirms that that self-determination is contagious, for the onset of self-determination claims in a country is strongly predicted by the onset of self-determination claims in the neighbourhood. The observations of the micro-regional dynamics in Eastern Europe and South Caucasus well-illustrate such a contagion – from Nagorno Karabakh to Transnistria, form Abkhazia and South Ossetia to Crimea and (partially) Donbas, and to a smaller extent, Gaugauzia. Rather unsurprisingly, Russia’s orchestrating or other-how instrumental efforts behind these processes have been disentangled and moderately well documented. With Putin’s Blitzanschluss of Crimea in 2014, the debate about the challenges of a weaponized ‘self-determination in the age of Putin’ (Simpson 2014) loom large – and not only in the context of lasting fears in the Baltics about the externally-strategized secession of Latvian Latgale or Estonian Narva provinces; the concerns grow in ‘old Europe’, too, especially after Russia’s considerable politically subversive effort was identified behind the 2017 Catalan referendum in Spain (Palmer 2017; Emmott 2017; Alandete 2017b; EFE 2018) and the ‘Brexit’ campaign in the UK, which, in a way, too, can be seen as a case for (a different but still a kind of) ‘self-determination’ – i.e. British determination to ‘depart’ away from Brussels and the EU’s institutional embrace. Importantly, one should, to a lesser extent, perceive such a subversion driven by the Kremlin as a hostile act strictly against respective nation-states, or at least nation-states alone (Cohen and Radin 2019) – such a weaponization of ‘self-determination’ processes in Europe targets the European Union and its transatlantic links, which stand in the epicentre of Russia’s fight against the liberal democratic hegemony of the Euro-Atlantic order. Bonet (2017) put it quite eloquently when referring to the Russian influence campaigns in Spanish Catalonia: ‘Russia’s official media speak about Catalonia, but they are really shooting at Brussels, using the referendum as ammunition’

The Russian uses of referenda as part of political warfare campaigns abroad are not limited to the cases of self-determination. Its uses span across a variety of deliberative democratic policymaking processes – from policy-consultative referenda, such as the 2016 Dutch referendum on the EU-Ukraine Association Agreement or the ‘Brexit’ referendum (Ostanin and Rose 2016), to electoral campaigns, such as the 2016 US presidential elections, German 2017 parliamentary elections (Applebaum et al. 2017), French 2017 presidential elections (Dearden 2017), etc. The evidence abounds that the ‘weaponization of referenda’ has meanwhile successfully broadened in its use as part of the hybrid warfare toolkit. NATO Parliamentary Assembly STC’s most recent report on Russian meddling in elections and referenda in the Alliance (cf. Davis 2018) draws on the collected evidence of the Kremlin’s past elections and referenda influence campaigns in the US, UK, France, Germany, Spain and the Netherlands, and argues that such interference operations pose a serious threat to the Alliance and its members, especially when seen against the broader efforts of Russia to divide, destabilise and otherwise undermine Alliance members.

Russia’s hybrid warfare proliferates, however, well beyond the weaponization of ‘self-determination’ and ‘referenda’ campaigns. It includes a range of activities in stirring up dissent abroad – from influencing campaigns to financial military and political support of local radical groups or insurgent forces. In this context, Afghanistan is yet another largely overlooked grey zone of Russia’s proliferating hybrid war against the West sought to undermine the latter’s global hegemony and resources in sustaining it, inter alia by provoking – mainly the US – to fight on several fronts (cf. e.g: Sazonov 2017). Casting a look at Afghanistan (again!) and actively courting the Taliban through arms supply and diplomatic conciliation amidst still designating it a terrorist group and domestically outlawing as such (cf. e.g.: Ramani 2019) has little good reason and military-strategic promise – if not considered against the Kremlin’s prima facie irrational (but no lesser deployed for that very reason!) strategy of inducing a ‘manageable chaos’5 , i.e. an operation in shaping a strategic environment conducive to Russia’s broader political warfare against the West. In the Kremlin’s forceful drive against the international liberal order and the ‘power of rules’, the strategic value of a spread of ambiguity, uncertainty, chaos and hesitation (be it via proliferation of grey-zone conflicts and hybression of sorts, weaponization of migration, populism or the rise of the so-called illiberal democracies, etc.) can hardly be overestimated (cf. e.g.: Tyushka 2018).

Reviving dormant ethnic-political tensions, sowing distrust, exaggerating tensions up to staging coups (such as the attended coup in Montenegro, cf.: Higgins 2016) is yet another modality of political warfare the Kremlin wages in the Western Balkans, in addition to the heating-up of separatist and revisionist movements (Bechev 2018).

Ironically enough, hybrid warfare campaigns can, too, spread to include deceptively ‘integrative’ agendas. As the pressure of Western sanctions and tensions between Russia and Belarus grow, the discussions on Russia’s possible hybrid invasion of Belarus have started to unfold among regional security scholars, especially after their joint 2017 ‘Zapad’ (‘West’) military drills (Wilson 2017) and more recent Kremlin’s calls for a closer integration between Russia and Belarus (Applebaum 2019).

Even though the prominence of Russia’s hybrid warfare in the region abounds in its scope and intensity, it would be wrongful to attribute all the endeavor and ‘brilliance’ in contemporary practices of hybrid warfare to Russia alone: a number of other state and non-state actors worldwide, unilaterally or collectively, resort to hybrid tactics in support of their diverse strategic goals – from China, India, Pakistan, Qatar or Iran to the US (cf. Figures 2 and 3, and Table 1 above). In the Middle East, Iran and Qatar come to the fore of attention. Dalton (2017: 312) posits that, for as long as the past three decades, Iran ‘has grown proficient at using hybrid-war capabilities and tactics to achieve its regional objectives’, typically operating below the threshold of conventional warfare, thus ‘using a blend of military and paramilitary tools, including proxy forces, missiles, cyber tools, maritime forces, and information operations to share and coerce regional actors to its advantage’. Supporting non-state actors, like Hezbollah and other proxy groups from Syria, Iraq, Afghanistan or Pakistan, forms part of the Iran’s regional leverage toolkit. In Asia and its regional security architecture, proliferation of hybrid warfare may, too, be fraught with systemic consequences. Niruthan (2016) contends that, already now, ‘[m]any of the conditions that breed hybrid threats are ripe for harvest in the Asian continent, with its ethnic conflicts, a vibrant tech industry, territorial disputes, and inconsistent rule of law’. Whereas the topic reappears more frequently in the discussions of China’s ‘legal alchemy’ and political subversion around the South China Sea dispute, potential cradles of hybrid warfare in Asia may also become Burma (Myanmar), Thailand or Pakistan, with the latter one becoming incrementally framed in the regional political discourses as both a target (Khan 2018) and a wager of hybrid warfare in its rivalry with India (AFP Kargil, 2014; Kumar 2017).

Evidently, the geography and uses of hybrid war(fare) manifest contagion effects, which remain underexplored in the subject-matter literature.

#### Researching hybrid war is good. Information war is a threat.

Alika Guchua 18, Scientific Researcher at Caucasus International University, 2018, “ASYMMETRICAL THREATS AND THE IMPACT OF HYBRID WAR ON GLOBAL SECURITY AND ROLE OF NATO IN ENSURING PEACE,” 2018, No. 2, Issue 11, pp. 214-224, https://anteportas.pl/wp-content/uploads/2019/03/AP.XI\_Guchua.pdf

Asymmetric threats

Against the challenges and geopolitical processes in the modern period world, research of the challenges coming from asymmetrical threats and hybrid warfare is very important. The world faces a number of challenges that cannot be solved without a united effort. Therefore, it becomes necessary to create alliances and enhance the effectiveness of international organizations. Coming from the current situation of today’s reality and geopolitical changes the role and the function of NATO is very important in world security issues. Since the establishment of the North Atlantic Alliance, ensuring collective defence and security is one of the main principles and purposes of functioning of this organization that require the Alliance to prevent the land, air and naval attacks with united forces, however, in modern times the Alliance faced new challenges that come from asymmetric threats and hybrid warfare.

The security trends play the great role in the process of forming a new system of international relations. In the past few years, one can often hear the reasoning that the nature of war in the twenty-first century has changed. Non-state structures even a century ago used partisan methods of warfare, and the beginning of the twentieth century was marked by the use of terrorist tactics.

Before we begin to talk about asymmetric threats and a hybrid war, it is important to consider what these two phenomena mean and what role they play in global security. During the consideration of the hybrid war, it is interesting to pay attention to the asymmetric warfare factor - asymmetric war represents such a war when the military powers of the opposing sides clearly differ from each other. The military tactics or the strategy used by them are very different from each other.

The term asymmetric warfare is used when describing situations such as guerrilla warfare, terrorism, insurrection and during such armed conflicts when regular military force confronts an irregular, ill-armed opponent.

The term became popular in 1975, when Andrew J. R. Mack, wrote in academic journal World Politics, "Why Big Nations Lose Small Wars," where he used an asymmetric war to determine the differences between important military forces among the parties involved. In the word "power" he meant the material strength, like a large army, good weapons, a developed economy, etc.

As for the connection of the asymmetric war with terrorism, there are different opinions on this issue. In today's world, asymmetric warfare is being increasingly considered as a part of the fourth generation war. Some believe that if the asymmetric war goes beyond the rules of war, it turns into terrorism. In addition, some believe that the asymmetric war is not connected with terrorism. They believe, because of the propaganda of the strong parties, it identifies the weaker party as bandits or terrorists. They also believe that the word terrorism is specifically used for political purposes because of its negative significance. One of the main security problems of the modern world is asymmetrical threats, such as international terrorism and transnational organized crime; Weapons, including weapons of mass destruction and its components; Also illegal drugs and drug trafficking; Human trafficking, cybercrime, and the fourth generation war. There are many other types of confrontations - rebellion, civil war, revolution, etc.

The tactical success of asymmetric wars depends on several components. On the example of technological advantage - if any party has a technological advantage, this can outweigh the enemy's numerical advantage. Neutrality of technological advantage is possible on important enemy facilities and with an attack on infrastructure. With attacking the electrical power lines or generators, roads, pipelines or water. In heavily populated places, such sabotage can greatly affect the morale and economics of people inhabiting the territories. The weaker side in such a war uses special tactics to cope with a strong opponent. You can break the rules of war and use them for your own good. The rules of war prohibits the use of a medical machine for asylum, an attack or an ambush, and the use of urban settlement for military bases is also prohibited. The weaker side uses such tactics with the hope that the opposing party will defend the rules of war and not attack the city2 .

The beginning of the 21st century brought about non-conventional security threats (they include natural disasters, drug, weapon and human trafficking, cyber warfare and piracy, etc.) which represent new challenges for those international organizations that consider maintenance of security and stability as their principal goal on either global or regional levels. The North-Atlantic Alliance has taken the responsibility for addressing these new challenges3 .

Today NATO provides its capabilities and resources to assist international and regional organizations in tackling crises and resolving a wide range of problems

Asymmetric warfare used to be determined as “a conflict including two states with different total military and economic resources”. However after 9/11 attacks the definition has been adjusted, Asymmetric warfare is now defined as “using inferior tactical or operational strength against the vulnerabilities of superior opponent to achieve the disproportionate effect with the aim of undermining [the opponent’s] will in order to achieve the asymmetric actor’s strategic objectives.”4

The problem of terrorism is not only the problem of a single country but also the first enemy of international security. The terrorist attacks of September 11, 2001 (9/11) led to a more clear perception of the threat of terrorism. Terrorism has become the most acute issue after this incident, and maintains the considerable attention of the international community until now.

After 9/11 terrorist attack, NATO instantly expressed support for U.S. For the first time NATO activated the Article 5, which envisaged the collective protection of member states at risk. The purpose of this action was not only America fighting against terrorism. Europe joined the events of 9/11. The fight against terrorism became the mainstay of EU member states.

While we start talking about the factor of hybrid war in the modern era, let us see what the existing theories and their authors are saying about the hybrid war. In general, there are two basic mental approaches around the hybrid war. Some researchers think that a "hybrid war" is a reality that needs to be understood. They think that this is separate from the traditional and non-traditional possibilities of creating a war, although it includes both. According to the second part of the researchers, the "hybrid war" by its content consists of the fact that it is not new for the stories of creating a war, does not need branches and is easily described with the help of comprehension of the historical perspective. In general, it can be said that the vast majority of researchers agree that in the form of creating a modern war, there are novices that need attention. The main question is how new this phenomenon is in the framework of the historical perspective.

At present, the term "hybrid war" has a significant place in the political dictionary. Over the past decade, a new military strategy has become more relevant in the world political arena.

In the Euro-Atlantic space, the number of conflicts that are not part of the Western category of war is growing. We can say that the analysis of these conflicts show the modern idea of a hybrid war, in which we see an intentional combination of forms of war to achieve strategic goals.

Modern American military analyst of conflicts, Frank Hoffman in various forms of analysis of hybrid threats defines as follows: "hybrid threats if the enemy at the same time uses conventional weapons, irregular tactics of terror-ism and criminal behavior, as well as a combination of military operations to achieve political goals."5

Military experts of the United States during the XX century introduced the concept of military planning together with the concept of "hybrid threats" and, consequently, the new concept of "hybrid wars" - a form of warfare that includes different composition, means, and level of training and characteristic of forces - was created. However, what makes a hybrid challenge the new phenomenon is the growing importance of non-military means. This is a modern form of war, which focuses primarily on achieving strategic goals without physical confrontation, especially at the initial stage of the conflict.

Conventional (regular) warfare is, according to NATO’s definition, warfare where regular opponents, officially enlisted as states, are engaged and regular tactics and activities are used, while respecting international treaties, conventions and laws.

Irregular warfare, according to available NATO’s definitions, represents a warfare that denotes a form of conflict, where one or more protagonists adopt irregular methods. Additionally, “irregular troops are any combatants not formally enlisted in the armed forces of a nation-state or other legally constituted entity.” Other definitions describe it as “a violent struggle among state and nonstate actors for legitimacy and influence over the relevant populations. Irregular warfare favours indirect and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary’s power, influence, and will. ”Moreover, irregular opponents are unlikely to adhere to recognized treaties and international conventions. On the other hand, they are likely to rely on local support, fight in the place they live and they are often hard to distinguish from local civilians. The irregular opponents’ tactic will often include undermining and eroding target’s will and determination. The tactic also includes avoiding regular decisive deployment of national forces, and if necessary, then preferably under the terms and circumstances chosen by the irregular opponents.

Hybrid warfare in NATO’s view is a violent conflict applying combination and simultaneous use of conventional and irregular warfare, involving both state and non-state actors, used adaptively in pursuit of their objectives and not limited to physical battlefield or territory. Each attack contains its own combinations and mutations of the two and targets further aspects of state and society to undermine it and reach its goals. Hybrid warfare can be employed in conflicts not only by states and armed forces but also by a variety of actors beyond the authority of states. (Such as terrorist or extremist groups.) Even though the phenomenon is hardly new, what is new and surprising is the “scale of use and exploitation of old tools in new ways.”6

**[Omit Fig. 1]**

Hybrid methods of warfare, such as propaganda, deception, sabotage and other non-military tactics have long been used to destabilize adversaries. What is new about attacks seen in recent years is their speed, scale and intensity, facilitated by rapid technological change and global interconnectivity. NATO has a strategy on its role in countering hybrid warfare and stands ready to defend the Alliance and all Allies against any threat, whether conventional or hybrid.

Highlights

- The primary responsibility to respond to hybrid threats or attacks rests with the targeted nation.

- NATO is prepared to assist any Ally against hybrid threats as part of collective defense. The Alliance has developed a strategy on its role in countering hybrid warfare to help address these threats.

- In July 2018, NATO leaders agreed to set up counter-hybrid support teams, which provide tailored targeted assistance to Allies upon their request, in preparing for and responding to hybrid activities.

- NATO is strengthening its coordination with partners, including the European Union, in efforts to counter hybrid threats.

- NATO’s Joint Intelligence and Security Division has a hybrid analysis branch, that helps improve situational awareness.

- It also actively counters propaganda – not with more propaganda, but with facts – online, on air and in print7 .

Hybrid threats include cyber-attacks, disinformation, economic pressure, the destruction of non-permanent armed forces and the use of regular forces, which is of military and non-military importance. The most important work of NATO is the prevention and destruction of hybrid attacks (the scale and frequency of which has greatly increased in recent years) and it does not matter whether it comes from government or non-state bodies. Hybrid methods first blur the boundary between peace and war and begin to be a problem for NATO. Since 2015, NATO has begun to fight with this warfare. To this end, NATO will prepare the Alliance and Allies to the extent that they can provide it all. For constant readiness, NATO continually gathers, exchanges and evaluates information to ensure any necessary activity. An integrated intelligence and security unit at NATO Headquarters assists this process. The hybrid analysis department provides maximum information on hybrid threats. Together with the abovementioned, NATO also supports allied in civic preparedness and response to chemical, biological, radiological and nuclear (CBRN) phenomena; protects critical infrastructure, strategic communications, and energy security, combats terrorism, and also provides cyber defense, which is very important. To implement all of the above, it is very important to conduct trainings and checks, which will make the fight against hybrid threats much effective

NATO can hold up hybrid threats much faster and more agile, and each time it improves preparedness for the fight and the decision-making process and the management of defense and control. It also shows that the Alliance is also strong in political and military efficiency and in a quick decision-making process. In the event that the struggle becomes impracticable, NATO, with its speed and flexibility, at any time and in any place protects its allies from any attacks.

To strengthen and improve the fight against hybrid threats, NATO continues to cooperate with Finland, Sweden, Ukraine and the European Union. The European Union and NATO have especially strengthened their cooperation against cyber-attacks and are successfully conducting this process.

For better experience, centres of excellence (international research centres) provide the alliance with more knowledge at the national or multinational level.

In October 2017, NATO Secretary General Jens Stoltenberg, together with the European Union Representative for Foreign Affairs and Security Policy / Vice President of the European Commission Federica Mogherini, opened the European Centre of Excellence for Combating Hybrid Threats in Finland, which supports 14 countries to improve their capabilities and preparedness to counter hybrid threats8 .

New Security Challenges: The Emergence of ‘Hybrid Threats’ as Challenges to Peace and Security

Multimodal, low intensity, kinetic as well as non-kinetic threats to international peace and security, including cyber war, asymmetric conflict scenarios, global terrorism, piracy, transnational organized crime, demographic challenges, resource security, retrenchment from globalization, and the proliferation of weapons of mass destruction were identified and labelled by NATO as ‘Hybrid Threats’, as threats ‘posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives’

Having identified these threats, NATO undertook work on creating a comprehensive conceptual framework, a Capstone Concept, which was to provide a legal framework for identifying and categorizing such threats within the wider frame of possible multi-stakeholder responses. In 2011, NATO’s Allied Command Transformation (ACT) supported by the U.S. Joint Forces Command Joint Irregular Warfare Centre (USJFCOM JIWC) and the U.S. National Defense University (NDU) conducted specialized workshops related to ‘Assessing Emerging Security Challenges in the Globalized Environment (Countering Hybrid Threats [CHT]) Experiment’.

These workshops took place in Brussels, Belgium, and Tallinn, Estonia, and aimed at identifying possible threats and discussing some key implications when countering such risks and challenges. The findings of the workshops were published in the ACT’s final report and recommendations in 2011.

Hybrid threats faced by NATO and its non-military partners require a comprehensive approach allowing a wide spectrum of responses, be it kinetic and non-kinetic by military and non-military actors. Such a comprehensive response will have to be in partnership with other stakeholders, such as international and regional organizations as well as representatives of business and commerce. However, due to a lack of financial resources in general, and an absence of the political will to create necessary ‘smart defence’ capabilities among its member states, NATO decided in June 2012 to cease the work on CHT at its organizational level while encouraging its member states and associated NATO Excellence Centres to continue working on hybrid threats9 .

At present, information warfare is the main component of the war, which means influencing the masses through access to the media, getting support for some idea and making the client's policy. Information warfare often includes informative, propagandistic, psychological, and cyber components and the characteristic of the "hybrid war" is the use of integrated financial resources, material resources and hidden military means.

A new type of war in the North Atlantic alliance, the "hybrid war" that unites all elements of a new strategy, is called tactics, when military facilities are not used. The war contains elements of propaganda and disinformation, as well as forced use of economic pressure and Special Forces. This kind of war is referred to as "soft power". Today, the main component of the war is "informational war", which means influencing the masses through access to the media, getting support for some idea and making a client's policy. "Informative war" often combines information-propaganda, psychological and cybercrime.

A vivid example of such a conflict is the Russian aggression against Ukraine. The appearance of Russian militaries in Crimea without the marking signs ("hidden faces, hidden management and controls") directly means the secretive use of Special Forces, which is one of the main elements of this kind of war. The use of such forces, which do not have any marks, in military opera- tions, allows Moscow to carry out an active campaign of rejection, aiming to mask its military intervention. Russian television is actively using militarist propaganda to mitigate and justify aggression

It is worth noting the cyber-attack on Ukraine. Russia's actions against Ukraine are a good example of how cyber operations can be integrated into conventional military operations. Cyber-attack and anti-state propaganda campaigns of the Russian-Ukrainian conflict were carried out by DDoS attacks against Ukrainian media and government organizations, as well as on NATO and NGO sites. In addition, Russian communications intelligence used the data on the Internet to determine the location of the Ukrainian military units in eastern Ukraine.

Former NATO advisor on security issues, General Frank Van Kappen, was one of the Western analysts who described the Russian-Ukrainian conflict as a "hybrid war" on 26 April 2014.

It is possible to say that the "hybrid war" theory of the Russian-Ukraine conflict has been created. This type of war has already been recognized as "hybrid war" - one of the major challenges, confirming a new strategy against the threats by NATO in December 2015. As NATO Secretary General Jens Stoltenberg said at a meeting of the NATO Foreign Ministers in Brussels, the Alliance will agree with the EU in implementing a new strategy, as the hybrid war contains both military and civilian elements. The emergence of a hybrid war as a new form of conflict fundamentally alters the existing landscape and provides many questions about the possibilities of security systems10 .

Finally, we can say that "Information War" is one of the most important threats of the XXI century, which threatens international security in addition to internal state relations. This can be used that support the recent history of the Russian Federation from the "information war" as the use of technology (2008) and Ukraine (2015-2016 years) against. Briefly, let's review the results of intelligence impact on the national security system of Georgia in the summer of 2008. Analysis of events allows us to assume that its northern neighbour used not only traditional ways of attack - by land, sea and air, but also implied the fourth, relatively new, but the most effective way of attack in terms of information, including cyber-space. According to the report published by the Ministry of Foreign Affairs of Georgia in August 2009, the Russian citizens and their sympathizers on 7-16 August 2008 carried out a coordinated attack that destroyed dozens of important web pages, including the web pages of the President, Defence Minister, National Bank of Georgia and other state agencies. Turns out, that cyber- space protection (including the threat of a timely response to the propaganda) in terms of intelligence and counterintelligence measures completely collapsed.

The stability of national security depends much on each individual component of international security. One of the major and general components in the world today are considered the danger coming from asymmetric threats and hybrid war, which seriously threaten the national security and strategic interests of the states. The world faces a number of challenges that cannot be solved without a united effort. Therefore, with the purpose of prevention of similar threats and minimization of the risks, it is necessary for states to take appropriate steps toward cooperation, where collective security is granted with big significance and the necessity for forming alliances, increasing the effectiveness of international organizations, defending the international security system and protecting of global security occur. NATO plays an important role in tackling existing threats, has a strategic concept and takes preventive measures to combat threats. NATO has a variety of approaches, which are brought forward in its new conceptual documents, to ease the existing challenges and threats.

Security is especially important in the era of globalization, when economization, democratization, informatization creates unprecedented opportunities for development, but at the same time makes the international relations system more vulnerable against challenges such as terrorism, weapons of mass destruction to use.

Conclusion

The increasing popularity of the use of asymmetric threats and hybrid operations in more and more parts of conflict areas rise questions how to adopt traditional Western conventional warfare so that it is able to face new challenges of the 21st century. The future conflicts will however no longer be possible to categorise only as conventional or irregular, state or non-state. NATO has mechanisms, means to combat actively asymmetric, and hybrid threats. The world is facing global threats, risks and challenges that make international security vulnerable with the development of new technologies. The development of technologies in the XXI century has brought many benefits to the society, but in terms of intelligence and "informational war" for its implementation, it has led to many threats. The security trends and new challenges play a major role in the establishment of a new system of international relations. After the Cold War, NATO's successful transformation and regulation of non-traditional security threats is the basic prerequisite for the globalization of the international role of the alliance.

Asymmetric threats and hybrid warfare affect the global security environment, which makes the global security environment vulnerable to modern threats. Despite global changes in the world, NATO has managed to establish peace and stability in the Euro-Atlantic area. After the end of the Cold War, when the main enemy of the Warsaw military bloc was disintegrated, there was the illusion that NATO had exhausted its function and could have dissolved. NATO underwent a transformation in the post-Cold War period, which significantly strengthened the Alliance and helped stabilize the balance of the power in the world. Today, NATO successfully cope with new challenges and threats of the 21st century and makes a significant contribution to the international security system.

### AT: Hybrid War K---Perm Do Both

#### “Hybrid threats” bring criticism of modern power into the open.

Maria Mälksoo 18, Senior Lecturer in International Security at the Brussels School of International Studies at the University of Kent, 2018, “Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO,” European Security, Vol. 27, Issue 3, pp. 374-392, <https://www.tandfonline.com/doi/full/10.1080/09662839.2018.1497984>

Conclusion

This article has brought the notion of OS to bear on the thus far heavily policy-oriented hybrid warfare literature. As hybrid threats epitomise ontological insecurity, NATO and the EU’s synergistic discourse and emerging practice on countering the hybrid menace emerges as an attempt at the institutionalisation of their organisational OS-seeking. Tackling the hybrid challenges of the day in apparent unison further provides NATO and the EU a silver lining of a tightened cooperation between the two organisations. Further research could map the complex interactions between the OS-seeking strategies of these distinct intergovernmental institutions and their member states/societies with regard to countering hybrid warfare. It would be interesting to investigate, for example, how the traditional lines of division within the European community along the more Russia-friendly and Russia-wary countries might tap into the institutional dynamics of hybrid threat management of the EU and NATO. Moreover, the newly established special sub-institutions to confront hybrid threats within the EU along with the organisationally unaffiliated Centre of Excellence could themselves develop their own identities, OS drives and placating routines, potentially generating organisational fragmentation and inter-agency tensions instead of bolstering the OS of the Union as a whole (cf. Steele 2017).

With regard to the ethical drawbacks of effective hybrid threat management, such an endeavour points at the problematic prospect of compromising the already fuzzy distinction between politics and war – as according to the hybrid warfare paradigm, all politics becomes reduced to the potential build-up phase for a full-blown confrontation. In that sense, hybrid warfare is close to the criteria of “minimal wars, which consist in merely threatening the enemy with negotiations held in reserve” (Clausewitz 1976, 604, emphasis in the original). The alleged “minimality” of such a way of warfare nonetheless has considerable potential to induce broad and deep securitisation of various public policy processes in the Western societies and their supranational organisations in question. Hybrid warfare and the emerging institutionalisation of its countering practices highlight the paradox of defending democratic security communities, as the efficacy of such defence might in fact be detrimental to some of the core organising principles of democracy.

An alternative approach would be to argue that hybrid warfare, and the countering practices it is generating, have simply brought the nature of the modern power out into the open. As Foucault maintains in his Society Must Be Defended, liberal “civil peace” must be understood as a secret form of war, for “war is the principle and motor of the exercise of political power” in general (Foucault 2003, p. 18). Viewed from such a perspective, hybrid warfare and its emerging management practices by the EU and NATO enable us to see what politics is allegedly all about anyway – “the continuation of war by other means” (Foucault 2003, p. 15). For the EU and NATO, hybrid warfare embodies not just the unsettling of the politics/war distinction but raises the fundamental question about the practical distinguishability of their physical and ontological security in the first place.

### AT: Hybrid War K---AT: Terminological Ambiguity

#### Hybrid war is not ambiguous, and there isn’t a universal formula to describe its contents.

Andriy Tyushka 19, Senior Research Fellow in the European Neighbourhood Policy Chair, 2019, “Hybrid War(fare): The Challenge of Contagion,” 2019, Torun International Studies, Issue 12, pp. 5–29, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-c63913a7-9115-4d4a-8c3e-a620eeb5d495

Since the early 2000s, the rise of the ‘hybrid warfare’ term can hardly go unnoticed. From a new term in U.S. military and operational code, introduced with the 2005 National Defence Strategy Review, to a consolidating phenomenon in strategic studies and a proliferating buzzword in public and political debates, especially in Europe, the notion of ‘hybrid warfare’ seems to be living a life of its own. Coined by Hoffman (2009) as a way to describe modern fanatical fighting styles, supported by new technologies and deployed in the shadow of state agency (no full deployments of army, no uniforms – and no need to obey the laws of armed conflict), the ‘hybrid warfare’ term is now used and abused in many possible ways – including the cases in which it is misleadingly equated with the idea of ‘hybrid war’, understood as something less than war. The lack of clarity as to what is what is particularly disturbing as the term(s) virally spread in public and political debates as well as academia. Hardly any security journal or a strategic studies event save an effort in addressing the ‘complexity’ of the notion. Some find it fancy and meaningless, some – revolutionary but evasive in its conceptualization (cf. e.g. a critique of the literature by Johnson (2018)). The term seems to be broad and flexible enough to encompass many things at once – and different things in different contexts, wherefore it is often used as a catch-all term for all non-linear threats. And yet, the idea is rather simple: modern technology has enhanced the known modes of warfare as well as it enabled the discovery of new battlefields, methods and ‘fighters’ – beyond armed troops. NATO’s 2014 Wales Summit declaration described ‘hybrid warfare threats’ as ‘a wide range of overt and covert military, paramilitary and civilian measures [that] are employed in highly integrated design’ (NATO 2014). As such, they ‘blend the lethality of state conflict with the fanatical and protracted fervor of irregular warfare’ (Hoffman 2009: 37). The notion is therefore not constrained to a particular set of fighting methods or a particular agent of war – it can equally be deployed by any state and non-state actor and will hardly be deployed in precisely the same manner twice – and, thus, can hardly be ‘calculated’. Critiquing Fox and Rossow’s (2017) attempt at ‘making sense of Russian hybrid warfare’ on their sixteen-page working paper published by the AUSA Institute of Land Warfare, Ricks (2017) laments that ‘[t]hey offer a series of unsatisfying summaries of other experts’ unsatisfying claims, and come up with an unwieldy version of “hybrid war = information operations + unconventional + cyber + conventional, spread out along an axis of covert and overt operations”’. This can be said about much of the literature on the subject trying to find and ‘patent’ the universal formula of hybrid warfare applicable in any context and in any part of the world – which does not exist, of course: every instance of this evolving warfare campaign has its specific sources, strategic and operational goals, battlefield(s) and tactics – all within a particular hybrid war strategy.

What can be said with (a greater) certainty, is that this twenty-first century art of warfare is multi-modal, multi-theatric and multi-agential. Hybrid wars begin long before the first shots are fired, if at all. With the use of both overt and especially covert means such as external financial and organizational support of democratic tools (referenda, elections, other public participation and influence campaigns) or less ‘visible’ information or cyber operations in target countries, the challenge is to instantly and firmly attribute an action, or a result thereof, to a hostile foreign agency. Both public debates, policymaking processes, digital transactions or physical battlespace may become theatres of warfare in hybrid strategies. In hybrid warfare, conventional military operations are not excluded – they just form the latest operation level. Before that moment, the place of uniformed soldiers is taken by soldiers without insignia (special forces, private mercenaries), astroturfed irregulars, troll and bot ‘armies’, cyber hackers, criminal racketeers, captured or corrupt elites, propagandists, psychologists and by manipulated media. In their 2012 book, Williamson Murray and Peter R. Mansoor define hybrid warfare as a ‘conflict involving a combination of conventional military forces and irregulars (guerrillas, insurgents, and terrorists), which could include both state and nonstate actors, aimed at achieving a common political purpose’ (Mansoor 2012: 2). Thereby, ‘[i]rregular forces need not be centrally directed, although in many cases they form part of a coherent strategy used to oppose an invader or occupation force’ (Mansoor 2012: 3). The range of ‘hybrid actors’ is, too, context-dependent and may include any combination from the variety of interpenetrated state and non-state agents – from insurgent or terrorist networks, organized crime groups, social groups (such as clans, tribes or ethnic groups), and ideologically or religiously motivated organizations, all of which may be backed covertly, or overtly, by states and/or legitimate businesses (Schroefl and Kaufman 2014: 867).

### AT: Russia K---2AC

#### Our securitization was good AND no generic links

Samuel Carruthers 19, Faculty of Social Sciences at Charles University, “Countering Disinformation: A Case Study of Government Responses to Russian Information Warfare,” Master’s Thesis, 2019, Institute of Political Science, https://dspace.cuni.cz/bitstream/handle/20.500.11956/110029/120343310.pdf?sequence=1

Ethics of Securitization

As discussed in the literature review, securitization is most often discussed as a ‘negative’ concept for several reasons. First of all, securitization argues that the normal democratic procedures for decision makers be abandoned in favor of a streamlined decision-making process handled by a small elite that dictate policy on security related issues. Critics assert that securitization is something largely inconsistent with the openness and accountability that liberal democratic systems value, therefore securitization is something ‘negative’ to be avoided in societies that place true importance on these values. But what if the issue being securitized is a direct threat to those very democratic procedures themselves. Are there issues that deserve to be securitized for the common good, and can government policies have a positive impact on society when these issues are securitized?

Experts on disinformation warn of the dire potential that such propaganda can have on a society, and argue that liberal democracies are especially vulnerable to them. New technologies have made the 21st century into a completely different type of information space than its predecessor. The internet has decentralized and democratized the flow of information to the point where somebody sitting on a laptop at home may be able to make the same impact with a blog as a major newspaper with an article. With less institutional control and traditional media gatekeeping on the flow of information, the internet is a truly democratic platform.148 These democratic processes; freedom of information, freedom of speech, freedom of the press, and free elections; are precisely what make liberal democracies so vulnerable to disinformation and propaganda. With knowledge of these asymmetric vulnerabilities, the Kremlin consciously aims “to take advantage of the free flow of information in a democratic society, the effect of that information on public opinion, and the electoral mechanisms through which public opinion determines a country’s leadership.”149

One foundation of a democratic society is the ability to make decisions in the public forum based on shared truth. When voters go to the polls, they may make a judgement on which candidate or which proposal they favor based on the information that they have consumed. Traditionally, they may differ on what course of action may be the best way to handle a problem, but there is an agreed upon reality that is a matter of fact; it is shared. Disinformation, from Russia and other actors hostile to the West, promotes falsehoods to the point where society cannot have a shared truth. Imagine four people each with a different source of news. One reads the New York Times, one watches Fox News, one reads Breitbart, and one watches RT. Each one of these people will not only come to radically different conclusions about what solutions are best for society, but also about what the basic facts of reality are in the first place. One person may be out on the streets protesting the disappearance and rape of a young Russian girl by Muslim migrants, while the next person may be aware that the story is a complete falsehood that never happened to begin with. Russian efforts in the EU show that these situations are not a hysterical fear-mongering reaction to new technologies and new sources of information, but that they are already a reality.

Disinformation creates a situation where people can have opposing realities because the information they consume is so radically different from that of their neighbor. Critical theory in international relations warns that securitization subverts democratic decision-making processes, but disinformation destroys these very democratic processes that are so fundamental for liberal democratic societies to function the way they are intended. It is impossible to imagine normal democratic processes solving these types of problems when those processes are being eroded by propaganda to the point where Western societies may no longer have normal democratic processes if this trend continues. In order to maintain these democratic norms, securitization may be a necessary process, even a ‘positive’ concept that can yield positive results and protect the democratic values that have propelled the European project into existence.

From the perspective of states, it is difficult to see why they would not wish to securitize the issue of Russian disinformation more. States tend to place an emphasis on matters of physical and territorial security over all else, which is why issues such as nuclear weapons, or rising military power in China, or international terrorism are prioritized in terms of security policy. States’ desire for physical security explains why these issues tend to be some of the most securitized political issues, with decisions made regarding military policy in Afghanistan by military panels rather than public referendums. Walt, arguing from the realist perspective, argues that states “place particular emphasis on the preservation of the state’s territorial integrity and the physical safety of its inhabitants.” 150 Material harm is of the utmost importance while more ethereal issues, like democratic procedures, freedom of the information space, and societal resilience towards propaganda are not prioritized in the same way. Disinformation has threatened some of the building blocks of democratic societies throughout the EU, and if these democratic systems fail, it isn’t difficult to imagine that physical security would come under threat as well. In the case of Spain, the issue of the Spanish government’s territorial sovereignty over Catalonia was attacked by Russian disinformation, exacerbating the political wounds of the independence referendum. The disinformation campaign questioned Spain’s fundamental right to exist in its current form, yet Spain did not place the integrity of their media space as an important security issue despite this. There needs to be a shift in the importance and value that European democracies place on the fundamental democratic principles that allow their system to flourish. They should be prioritized with the same importance that states place on more traditional measures of power. Securitization of disinformation with the liberal democratic system and democratic processes themselves as the referent object, has the potential to have a more ‘positive’ outcome than emphasis on hard power, or immigration, or other issues that contribute to the ‘negative’ conception of securitization.

Successful Securitization and Societal Resilience

In the case studies it is clear that some European countries have securitized Russian disinformation while some have not. Namely, the United Kingdom and Lithuania have successfully securitized disinformation, while Spain, Germany, and the supranational institutions of the EU have not securitized disinformation. Those that have not securitized, have identified Russian disinformation as a perceived security threat and have several securitizing actors currently at play. The potential audiences of the securitizing speech acts, those within the security apparatus, NGOs, think-tanks, and even the wider public of these countries have accepted that Russian disinformation is a security threat that warrants greater action by their governments. Thus far, they have not taken measures that could by any means be considered extraordinary, having allocated a relatively small number of resources and minimal effort towards combating disinformation, and therefore cannot be considered to have securitized the issue. These countries, and the EU, are possibly in the early stages of the process of securitization, though this does not necessarily mean that they will complete the process by taking more extraordinary measures against disinformation. In fact, there could be a reversal and disinformation could slip back into the realm of normal politics and become desecuritized.

Some clear trends emerge in the countries who have successfully securitized disinformation. First, propaganda narratives have a weaker effect on society when disinformation has been securitized, failing to have their desired impact and cause major rifts in the public. They also show that securitization of disinformation is possible without implicitly violating democratic norms of freedom of speech and open access to information. This becomes clear in looking at the contrast between Lithuania’s countermeasures against disinformation compared to those of Germany and Spain. In Germany, the Lisa case was dealt with almost exclusively via the normal criminal and legal channels, with the police investigation into Lisa’s accusations of kidnap and rape by migrants and police handling of most public statements related to the controversy. 151 They have begun to enact minor laws that aim at punishing hate speech and disinformation when posted on popular social media platforms as well.152 Spanish authorities have started task forces devoted to alerting the national government when disinformation narratives start to dominate a story online. 153 Spanish and German officials at the higher levels of national authority in their respective foreign and defense departments gave minimal statements regarding the controversies, and have preferred to continue dealing with Russia through dialogue over more overt confrontation that could complicate communication. Both Germany and Spain have taken a more reactive approach to countering disinformation, choosing to deal with it on a case-by-case basis as an incident unfolds.

Lithuania has taken similar messages to alert national authorities on dangerous narratives as they develop online, but it has also taken extraordinary measures that encompass a broader scope. The Lithuanian government has supported efforts at every level of society; political, economic, educational, and cultural. 154 Their wide spread programs focus not only on dealing with each case as it emerges, but also on strengthening the fundamental resilience of society at the source through teaching media literacy in secondary schools, funding Russian language media for the susceptible minority group, and sensitizing the public to the dangers of propaganda by making disinformation a security issue linked to the physical security and existence of the state.155 Their bans on Russian media channels during disinformation campaigns, while possibly construed as violations of a free press, are necessary to prevent media from spreading out right falsehoods. The news media, both Lithuanian and Russian language, should be held accountable and has a responsibility to act as a gatekeeper of the truth. Many media channels in Lithuania have voluntarily chosen to follow such a route, choosing not to report on ‘fake’ news stories that can be detrimental to society by becoming ‘real’ news through regurgitation by legitimate media outlets. It is important not to confuse the right of free speech of an individual with that of a news organization with ties to a foreign country, and such acts should not be considered violations of democratic norms when it comes to protecting the fundamental values of democracy.

The countermeasures taken by a country undoubtedly play a role in the impact disinformation narratives may have in that country. With Lithuania’s ‘successful’ securitization of disinformation, fake stories and attempts at propaganda have often fallen on deaf ears, with little real success. Lithuania’s overarching, comprehensive strategy at countering disinformation is the reason the NATO rape allegations failed to cause a large disruption in the news cycle.156 This strong contrast is seen with Germany, where the story of a rape by migrants of a young Russian girl caused an uproar and led to protests in Berlin and a diplomatic row with Moscow. 157 Spain also fell short, with Russian disinformation exacerbating a contentious independence referendum in Catalonia and influencing public opinion at home and abroad on the status of Catalan autonomy. Government policies that fail to securitize disinformation and alert society to the dangers of propaganda lead to false stories having explosive consequences.

Both Spain and Germany’s strategies of dealing with disinformation narratives as they arise is simply not effective enough. The state can spend time and resources trying to discredit every fake news story that finds its way to the public forum, but there will always be one to take its place. It is like fire prevention; a fire alarm can be an important part of fire prevention, alerting the fire department to come extinguish a blaze. But there are more important measures as well, such as building structures with fire resistant materials, or teaching people what to do in case of a fire. These types of continuous measures, like the policies Lithuania pursues, make society more resilient and prevent disinformation from causing a fire in the first place.

Policies aimed at improving societal resilience towards disinformation are being utilized in other countries with successful outcomes as well. Latvia uses a sweeping media literacy program from an early age to improve critical thinking in its citizens.158 Finland, a country with a long history of hostility with Russia, uses similar programs, emphasizing not only the need to publicly correct false narratives, but also the importance of creating a positive counternarrative to disinformation that is repeatedly applied to offer an alternative vision.159 These countermeasures only appear in countries that have securitized disinformation, as Finland and Latvia have similar histories as Lithuania and treat disinformation in similar terms, and they are much more promising than government authorities attempting to play catchup with internet trolls and false stories.

Internationalization of Countermeasures

Another key conclusion comes from the other case of successful securitization in the United Kingdom. The UK, in its securitization of disinformation following the assassination attempt on Sergei Skripal, internationalized the threat by creating a set of countermeasures that could be implemented along with its allies. The UK successfully convinced 20 allies to expel Russian diplomats in a coordinated effort at punishing Putin’s regime for the incident and the subsequent disinformation surrounding it.160 Theresa May, as a securitizing actor, not only convinced her public in the UK of disinformation as a security threat, but convinced the international community that such behavior “threatens the security of us all.” 161 Compared with the minimal Spanish attempts at coordinating counter disinformation at the EU level, and German attempts to keep the Lisa Case under the authority of Berlin’s police department, British efforts at securitizing their incident by bringing it to the attention of the international community and launching a unified response were highly successful.

This lesson of internationalization should be critical for the EU to deal with disinformation. Securitization needs to take place not only at the national level of member states, but also at the supranational level of the EU as an institution. The EU itself is under threat of Russian disinformation just as much as individual member states, with experts warning of further regionalization of Europe and the EU after Brexit. In this critical time for the continued existence of the EU, the threat of disinformation “requires new international instruments to manage it.” 162 Thus far, member states have shown a preference for taking individual routes in order to deal with disinformation. The importance of joint initiatives could be especially important during elections, a time in which the ability of national and EU authorities to cooperate is critical. During the European elections of 2019 for example, consisting of four days of simultaneous elections across 28 individual member states, “the failure of one government to properly mitigate disinformation efforts threatens the credibility of the entire electoral process.” 163 This problem of coordination cannot be understated, as some countries do not even have their own systems in place to monitor disinformation, allowing “local and national actors to spread fake news more freely” and leaving these countries defenseless against propaganda.164

It is essential for the EU to act as a bloc and start joint initiatives to counter disinformation. Russian efforts, as shown in the case studies, are not exclusive to one particular area of Europe, but threaten all member states. Issues Russia chooses to target; the migrant crisis, espionage, the use of chemical weapons in a member state, the solidarity and legitimacy of the NATO, and even the territorial sovereignty of some countries; should alarm every single member of the EU. These issues are not unique to one country, but they are issues that countries even outside of the EU are currently confronting. Europe is targeted as a bloc, and therefore it should respond as a bloc. Such a response, as seen in with the UK’s diplomatic expulsion, has a larger impact as a bloc rather than individually. Division will only encourage more provocations. Acting on a unified front in securitizing disinformation and reacting with countermeasures will do much more to potentially deter Russia from continuing down the same path in its relations with Europe. The EU needs to stop hesitating, and start throwing its full weight on the economic, political, and informational fronts.

‘Positive’ Securitization

The two trends discussed in the sections above also show that disinformation can be securitized without wide violations of democratic norms and exclusionary tactics towards Russian minorities in Europe. By arguing for securitization, this paper is not arguing that democratic principles should be thrown out in favor of extraordinary measures that subvert the democratic process, indeed the democratic process is of the utmost importance because these principles are the referent object of a European push to securitize disinformation. And according to polls in all of the countries involved in the case studies and the EU as a whole, the general public agrees that disinformation constitutes a security threat that could be detrimental to liberal democratic norms. Efforts like media literacy, cooperation with news organizations, and comprehensive strategies that deal with disinformation at every level of society are still extraordinary without necessarily violating democratic norms. These policies aim to sensitize the public to disinformation. They do not aim to monitor the public in a surveillance state and punish individual views that are unfavorable to European states. On the other hand, these policies are not afraid to prevent large news outlets from spreading lies that harm the ability to make democratic decisions based on shared truths. Diplomatic expulsion and unprecedented international cooperation on information issues are extraordinary measures taken without abuse of state power as in the War on Terror. Policies that aim to provide alternative news sources to Russian speaking minorities in Europe are not exclusionary ‘othering,’ but are inclusive and offer a broader, diverse, and more positive view of the Russian diaspora than as a monolithic fifth-column prone to side with Moscow and Putin’s regime over their new homes. These policies need to be inclusive to mitigate the risk of disinformation and the subsequent disillusion with European governments. A conscious, just policy of securitization of disinformation must take democratic principles, inclusion of diverse viewpoints, and the treatment of Russian minorities into account while avoiding the misuse of state power in order to succeed.

### AT: Russia K---AT: Threat Construction

#### The threat of hybrid warfare isn’t constructed---statements by Russian military officials prove the accuracy of our securitization

Lesley Kucharski 18, Research Assistant for The Center for Global Security Research, Lawrence Livermore National Laboratory, “Russian Multi-Domain Strategy against NATO: information confrontation and U.S. forward-deployed nuclear weapons in Europe,” 2018, https://cgsr.llnl.gov/content/assets/docs/4Feb\_IPb\_against\_NATO\_nuclear\_posture.pdf

\*IPb= informatsionnoe protivoborstvo=Russian information warfare

While traditional military measures are still considered the hallmark of inter-state conflict, Russian strategic thinking is increasingly highlighting the strategic importance of non-military, asymmetric, and indirect measures, including military and non-military IPb operations, in its multi-domain approach to conflict in the 21 st century. According to the Chief of the Russian General Staff, Valeriy Gerasimov, IPb is the only means of conflict resolution which spans across all stages of modern inter-state conflict and encompasses both military and non-military means (see Figure 2).23 The complexity of its role further increases during the initial stages of kinetic conflict operations. Reflecting a desire to minimize military confrontation during these stages, the ratio of non-military and military measures is described as 4:1.24

The novelty of Gerasimov’s perception of modern conflict (often described as the Gerasimov Doctrine) and the role of information in conflict resolution should not be overstated.25 The literature on Russian IPb emphasizes that contemporary information operations demonstrate that “the Kremlin is falling on a time-honoured strategy in its propaganda war.”26 Indeed, Russian leaders have operationalized information for strategic purposes since at least the Revolution. The Soviet government developed and systematically applied active measures and deception techniques that were intensive, persistent in times of war and peace, worldwide in scope, and centrally coordinated in a way that was not mirrored by Western governments.27 Informational psychological operations were coordinated by the political leadership and implemented by the state security apparatus, specifically the KGB (and its predecessors) and to a lesser extent the GRU, both domestically and internationally.28 Initially these operations were orchestrated on an ad-hoc basis, but by the late 1970s, an institutionalized system for coordinating and implementing them had been fully established. These overt and covert, non-military and military information operations were referred to by Soviet intelligence services as active measures. In 1982, the CIA described active measures as “an unconventional adjunct to traditional diplomacy. They are quintessentially an offensive instrument of Soviet policy.”29

The 1970s saw an organizational restructuring within the KGB and CPSU that signified an increase in the perceived strategic importance of active measures. According to a Ladislav Bittman, a former active measures agent for Czechoslovak intelligence (one of the most successful and loyal satellites of the KGB) who defected to the West, this organizational change was the result of an evolution in the perceived strategic importance of active measures that unfolded in three stages after World War II.30 In the first stage (1945-1948), active measures were characterized by an ideological emphasis on communism. In the second stage (1948-1959), the Soviet Union sought to increase the efficacy of active measures by making them appear more objective. To achieve this, the Soviet Union dialed back the overt ideological emphasis of its propaganda and used communist front organizations and Soviet satellite intelligence services to conceal its role in coordinating active measures.

Bittman notes that the Soviet government valued active measures as secondary to intelligence collection in the first and second stages and that this hierarchy of values visibly reversed in the third stage, which began in 1959 with the establishment of a department of active measures within the First Chief Directorate of the KGB. Many Soviet satellite intelligence services soon established similar departments which carried out orders from the KGB in addition to their own operations. Throughout the 1970s the Soviet government formally established an institutionalized structure for coordinating and implementing active measures (see Figure 3). This process began in 1970 when the active measures department of the KGB was elevated to a special service called Special Service A within the First Chief Directorate. Special Service A was responsible for carrying out active measures which were coordinated by the International Department (ID) of the Soviet Communist Party (CPSU). The ID assisted the Politburo in coordinating policy by liaising with the Ministry of Foreign Affairs, military, Academy of Sciences, the KGB, and non-ruling foreign communist parties.31 In 1978, the CPSU established another department for coordinating active measures: The International Information Department (IID).32 The IID was responsible for improving the effectiveness of Soviet propaganda abroad and improving treatment of foreign affairs by domestic media. Service A of the KGB managed the implementation of active measures coordinated by the IID as it did for the ID.

When exploring the causal mechanisms behind the institutionalization of active measures, one cannot overstate the influence the anti-war movement in the United States during the Vietnam War had on Soviet strategic thinkers. The movement demonstrated the potential efficacy of exploiting peace movements and public opinion in democratic societies to achieve political and security objectives.33 The foundation for this strategy was embedded in Bolshevik and then Soviet strategic thought which embraced the Marxist-Leninist notion that the struggle for peace is constant and characterized by conflict.34

This same notion of constant conflict is reflected in Gerasimov’s chart, particularly with respect to the role of IPb, since it is the only means of conflict resolution which is applied across all phases of conflict. The role of IPb in the Gerasimov Doctrine should therefore be interpreted as an evolution enabled by technological innovation, globalization, and the changing nature of conflict rather than a revolution in Russian strategic thinking about conflict.

Contemporary Russian strategic thinking about IPb developed within the body of thought known as New Generation War [voyna novogo pokoleniya], or NGW. Sergei Chekinov and Sergei Bogdanov published the seminal article on this concept in 2013. Entitled “The Nature and Content of a New Generation War,” the piece describes thinking within the Russian Ministry of Defense about the nature and content of warfare in the 21st century as well as how to prepare for and emerge victorious from it. 35 NGW emphasizes the growing importance of non-military, asymmetric, and indirect means of conflict resolution over traditional military methods.36 The theory of victory reflects an effort to achieve reflexive control [refleksivnoe upravlenie] without resorting to the military subjugation of the adversary.37 Under NGW, traditional kinetic military measures are used only after non-military measures and non-kinetic military measures fail to achieve strategic objectives or de-escalate a conflict. Figure 4 provides a graphical illustration of NGW and the Gerasimov Doctrine.

Dima Adamsky provides a useful description of Russian NGW strategy using Western nomenclature while avoiding the cognitively and conceptually problematic terms such as hybrid warfare. Borrowing from the body of thought on cross-domain deterrence, he develops a concept called Russian cross-domain coercion. Cross-domain coercion “refers to the host of Russian efforts to deter and to compel adversaries by orchestrating soft and hard instruments of power across various domains, regionally and globally.” 38

NGW first arose as a way to think about Russian military policy in light of U.S. advances in high-precision, non-nuclear military technology and its impact on the nature of conflict in the 21st century. 39 U.S. operations in the First Gulf War and NATO operations in the Balkans during the Yugoslav wars were perceived by Russian strategic thinkers as a watershed in the evolution of conflict. The advanced military technology utilized by the U.S. and its allies allowed them to carry out military operations remotely and with high precision, thereby decreasing the need for the type and level of mobilization characteristic of previous conflicts of the 20th century while simultaneously increasing U.S. and NATO power projection. Russia, which was suffering through an economic crisis after the collapse of the Soviet Union, was not in a financial position to develop symmetric countermeasures to U.S. advancements in non-nuclear military capabilities. In light of this economic disadvantage, Russian strategic thinkers sought to conceptualize a theory and develop a strategy for countering U.S. conventional superiority using asymmetric, including non-military, and less costly methods.40 Chekinov and Bogdanov note that the importance of this intellectual effort was highlighted by President Putin during a speech to the Federal Assembly in 2006 when he remarked: “We must consider the plans and development trajectories of the armed forces in other countries. We must be aware of perspective innovations. However, we must not chase after quantitative indicators…Our response must be based upon intellectual superiority. It will be asymmetric and less costly.”41

Justification for the informational component of NGW was provided by the collapse of the Soviet Union, the Color Revolutions, particularly those in the post-Soviet space, and Arab Spring.42 Chekinov and Bogdanov argue that U.S. information warfare techniques were a major factor contributing to the collapse of the Soviet Union.43 The perceived effectiveness of these techniques increased with the development of the Internet and social media. Russian strategic thinkers expressed alarm at the role of the Internet as a vehicle for undermining regime stability in the countries affected by the Color Revolutions and Arab Spring. They were further alarmed by Western financial, informational, and special operations support for anti-regime NGOs and political parties/movements in those countries. Such support, they contend, is a form of hybrid warfare that constitutes a violation of national sovereignty and is thus illustrative of Western aggression.

While condemning the use by adversaries of informational and other non-military, indirect techniques to undermine regime stability, Russia recognizes the strategic significance and costeffectiveness of such efforts in 21st century conflict and therefore incorporated them into its own strategy. Reflecting upon Western involvement in the conflicts in Yugoslavia, Iraq, Libya, Tunisia, Syria, and Ukraine, General Alexander Dvornikov, Commander of the Southern Military District and Commander of Russian Armed Forces in Syria when Russia began its military intervention, observed: “Now, aggressor states achieve geopolitical goals through a complex of non-military means which in several cases significantly exceed the effectiveness of military means. The primary objective is not the physical destruction of the adversary, but rather his complete submission to your will.”44 He further noted: “Modern armed conflict is acquiring a vast array of forms which, depending on the region and concrete situation, integrate separate elements into a unified approach. We [Russia] have taken account of this history, gained useful insights, and applied them to our operations in Syria.”

NGW identifies IPb as the primary tool in the Russian military and foreign policy toolkits for achieving victory in modern conflict as described by General Dvornikov, i.e. the submission of the adversary to one’s will rather than his complete military destruction. According to Chekinov and Bogdanov, “the means for exerting informational influence have reached a level of development whereby they are capable of resolving strategic objectives.”45 They further note: “In the ongoing revolution in information technologies, information and psychological warfare will largely lay the groundwork for victory.” Some Russian strategic thinkers predict that military actions in the information space will become the “deciding factor” in armed conflict.46

### AT: Russia K---1AR

#### Securitization of Russian disinformation is positive

Samuel Carruthers 19, Faculty of Social Sciences at Charles University, “Countering Disinformation: A Case Study of Government Responses to Russian Information Warfare,” Master’s Thesis, 2019, Institute of Political Science, https://dspace.cuni.cz/bitstream/handle/20.500.11956/110029/120343310.pdf?sequence=1

\*ableist language changed

Conclusion

This thesis aimed to identify similar processes occurring throughout the EU by analyzing how four individual member states have approached the issue of disinformation. In looking at incidents of disinformation in the UK, Germany, Lithuania, and Spain, research was conducted to analyze the incidents themselves and how governments responded, placing that response into the wider context of securitization within those countries. It is clear that there is an ongoing process of securitization taking place in Europe around the issue of disinformation. Not all countries researched have demonstrated that disinformation has been fully securitized, but every country had elements of securitization taking place, such as securitizing actors and speech acts meant to draw attention to propaganda as an existential security threat. While these countries did show the initial factors in securitization occurring, they chose to deal with disinformation through the route of normal politics rather than extraordinary politics. It can be concluded that the level of securitization of Russian disinformation within a society, that is the treatment of propaganda and false narratives as a security threat and how deep a country is within the process of securitization, played a direct role in shaping the policies those countries pursued in order to counter disinformation.

Examining the different cases, the research showed how history, experience, and threat perceptions related to Russia influenced securitization of disinformation. The United Kingdom securitized Russian disinformation in the aftermath of a catalyst event, the attempted assassination of former GRU agent Sergei Skripal and the subsequent disinformation campaign in its aftermath. The UK government propelled disinformation to extraordinary politics in its diplomatic expulsion of Russian diplomats coordinated with its allies. Lithuania securitized Russian disinformation over a long period of time because of its complex history with Russia and the Soviet Union, and its experience of a slow barrage of disinformation since it regained independence. Due to decades of experience, Lithuania pursues a more comprehensive strategy at countering disinformation, which seeks to address the threat at multiple levels of society and multiple stages as false-narratives spread.

It was clear that other countries, and the EU as an organization, had not fully securitized Russian disinformation, although they showed signs they were in the process of securitization. Germany, in response to a young girl’s explosive accusations of rape in the context of the migrant crisis, showed a clear preference for dealing with disinformation through the normal political channels of Berlin’s police department. Spain took minimal responses through its foreign and defense ministries and is still in the early stages of instituting policies aimed at alerting the government to disinformation narratives. As a bloc, the EU also failed to enact extraordinary policies to counteract disinformation from Europe’s Eastern neighbor, with a lack of coordination between the individual member states and the supranational EU bodies.

While some countries have securitized disinformation, other have chosen a different route, and we can see how the different policies enacted by these countries can either protect society or make society more vulnerable to disinformation. Those countries that have securitized disinformation have also had the most success in countering it. Continuous policies that not only track disinformation narratives and discredit them as they emerge on a case-by-case basis, but also build resilience at the source through policy efforts in the social, cultural, educational, and political realm have proven more effective. Media literacy, Russian language programming, and public statements exposing false stories can all have an impact. Disinformation narratives have often failed to cause the same explosive consequences in those countries that have instituted comprehensive strategies to counter it. Internationalization of counterdisinformation policies, seeking solidarity and joint initiatives with like-minded allies, has also proven more effective cultivating societies that are less vulnerable to fake news. Diplomatic expulsions, online tracking, and coordinated alert systems have the potential to ensure that the more vulnerable countries in the EU do not let disinformation exert influence on political processes and thereby endanger the bloc as a whole.

This paper has also argued against ‘negative’ conceptions of securitization in relation to the issue of disinformation. It has warned that disinformation is indeed a security threat to liberal democracies in the West, with its ability to destroy foundations of shared truth and potentially ~~cripple~~ [destroy] democratic decision-making processes. While critical IR theorists believe securitization should be avoided to protect openness and accountability, and frame the process in a negative light, this paper has argued that securitization is a necessary protective measure and does not inherently lead to abuse of state power. Policies pursued by the case study countries that have successfully securitized disinformation prove that while still extraordinary, countermeasures against disinformation do not necessarily need to violate the democratic values they are meant to protect. These policies do not need to be exclusive towards Russian minorities, but can be inclusive and contribute to public life. If European countries and the EU as an institution value the democratic principles that govern their societies, a conscious, successful securitization of disinformation may be beneficial and even have ‘positive’ results. Viewing disinformation as a national security threat is the path forward for the EU to respond to Russia.

### AT: Psychoanalysis

#### Can’t scale up psychoanalysis – sweeps historic and cultural forces unique to state political units under the rug

R.D. Hinshelwood 16, Professor of Psychoanalytic Studies at the University of Essex, 5/11/2016, Reflection or action And never the twain shall meet, https://freudconference.wordpress.com/2016/05/11/reflection-or-action-and-never-the-twain-shall-meet/

There is a major problem in using psychoanalysis in political activity. The unconscious individual influences and the external social ones are essentially different categories, and can be bridged conceptually only with some difficulty. I have been struck for some time by the conceptual divergence. In 1996, making an attempt to understand the convergence between a social (contemporary Marxist) explanation and an internalist, psychoanalytic explanation of human personality and experience, I noted that both paradigms are avowedly materialist; so,¶ Economic activity and bodily experiences create separate theories [but] they also generate separate superstructures – the world of social relations and the world of object relations respectively… [T]he two superstructures converge. They lean together and coincide At certain points, we have dealt with three of those points – oppression/repression, alienation/depersonalisation and commodity/identity (Hinshelwood 1996, p. 100-101).¶ In this Chapter, I return to this paradigm, and take further the alienation/depersonalisation point of convergence. The dialectical relations can be unpacked as several interactive cycles,¶ Group dynamics and the Labour Party¶ Back in the 1990s, I was part of a group that worked out some ideas which we might take to the Labour Party. You may remember that the dying regime of the Conservatives, Mrs Thatcher and John Major was hanging on, and with the election in 1997 coming up, the Labour Party was desperate to convince the electorate of its better policies. The idea was whether we could give an account of group dynamics which might be helpful to Labour to understand the way to create a more democratic society. At the time Labour were talking about ‘the third way’; somewhat vague, but it appeared that it might promote more measured attitudes in Society suggestive of depressive position thinking – ambivalence, considerateness towards everyone, and generally a reluctance towards the unrealistic perfectionism of ideologies. It seemed there could be a match between the political rhetoric and the study of unconscious group processes. In the event when we met a couple of people at Millbank, it was clear they were politely indifferent to what we were trying to present. Their interest was whether we had the secret of how to influence the electorate to vote for Labour. They wanted advice on their marketing. There seemed a radical disconnection between our earnest views about a more mature society, and their wish for effective marketing.¶ I have thought, over the years, about our naïvety. Obviously there is a potential for psychology to be used as a social and public instrument for manipulation, and later, I came across the writing of one of the founders of marketing and public relations, in the US back in the 1920s. He wrote,¶ If we understand the mechanism and motives of the group mind, is it not possible to control and regiment the masses according to our will without their knowing about it? (Bernays 1928, p, 71).¶ and¶ The conscious and intelligent manipulation of the organized habits and opinions of the masses is an important element in democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country (Bernays 1928, p.37).¶ I find this unpalatable. Shamefully, this author, a founder of this ‘invisible government’ as he called it, was Edward Bernays, Freud’s nephew. He, like Freud, was interested in the ‘unseen mechanisms’ at work in individuals – but for different purposes. ¶ Political change and psychoanalytic change¶ The aim of psychoanalysis is to change things. That is what patients want help with. The aim of politics is also to change things. But the changes, and how they are brought about, are completely different. Is that difference bridgeable? Influencing a patient towards some healthy state, and doing the same for society, shouldn’t be impossibly different. After all a society is made of people. So what really is the difference, and how can one inform the other?¶ Practising psychoanalysts address the internal unconscious factors that determine an individual’s personality – and how the individual is captured and controlled by them. On the other hand, political attitudes and actions are socially generated, arising, many would say, from the economic system of production. The individual is located at the junction of these two sets of influences, one from inside and one from outside. If someone has a phobia for spiders, he is driven by internal factors (his unconscious imagining, say, that the web-like embrace is a controlling mother). If someone drives his car on the left-hand side of the road, it is from social forces – the highway-code, police patrol cars, etc.¶ These are inherently different kinds of influences. How do social and unconscious determinisms fit together? Edward Bernays decided it is simple, the external social category is used to manipulate the individuals’ interior unconscious choices. Well…. for me that is not good enough, and I am interested in whether there are other ways by which these two categories of influences can be combined in our understanding). ¶ Interpreting society!¶ I claim we need to find models of interaction between social relations and psychodynamics. It is, otherwise, so easy for us, psychoanalysts, to approach society or social institutions as if they were individuals. To equate a social organisation with the individual mind risks leaving out the very valid social, historical, political forces that act on organisations, create cultures and induce or enable individuals to collaborate unconsciously, as well as consciously, with each other.. ¶ I am thinking of the campaign started by psychoanalysts in the 1980s, Psychoanalytic Psychotherapists against Nuclear War (PPANW). Led by Hanna Segal’s especial interest, expressed in her paper ‘Silence is the real crime’ (Segal 1987), the individual defence mechanisms she suggested seemed to be simply aggregated, and she talked of regression during wartime from depressive position to paranoid-schizoid functioning. The campaign remained largely ineffective, so, it seemed there were serious limitations to this kind of individualistic political approach –interpreting a supposed unconscious as if it were an individual unconscious. The political problem only disappeared with a political solution – the collapse of the cold war in 1990. I would suggest that attributing individual dynamics to social and political issues risks psychoanalysis becoming irrelevant to social scientists and politicians.

#### Psychoanalytic insights can only apply to the single person being analyzed

Adam Rosen-Carole 10, Visiting Professor of Philosophy at Bard College, 2010, “Menu Cards in Time of Famine: On Psychoanalysis and Politics,” Psychoanalytic Quarterly, Vol. LXXIX, No. 1, p. 218

Second, the structural-epistemological problem is that, if psychoanalytic practice is not to be theoretically heavy-handed, then psychoanalysts can only know what individuals within analysis can know, and if social relations are reified, then there is a socially imposed limit to the insights achieved and future prospects delivered via analysis. If social objectivity is dissimulated and mystified, that is, if the structures of our interdependence are socially opaque and the forces organizing modern social life are self-obscuring, then this reification is bound to be reproduced in the source material of analysis, that is, in the analysand’s self-experience. So, when the analyst facilitates the analysand’s freedom to experience, think, feel, and ultimately commit herself otherwise, all he really can do is help the analysand, say, commit herself to forms of self- and world relation that appear less injurious or more livable *to her*, but what appears less injurious or more viable will in all likelihood be limited to that which *can appear so* from the historically sedimented purview of a more or less bourgeois, self-interested, rights-bearing being. That is, what becomes available via analysis is that which can become available to the sociohistorically positioned analysand, and not only is there nothing psychoanalysis can do to get around this, psychoanalysis is not even in a position to shed light on the problem without delving into social theory and thereby abdicating its mandate to tarry with the problems and issues that the analysand experiences as at the heart of her predicaments. Analytic practice is caught in a double bind: as it seeks the emancipation of the analysand, either it is forced to become politically didactic and consequently counterproductive (or at least problematic qua analysis), or it promotes the extremely limited forms of emancipation imaginable by a typical bourgeois subject—and so it should be no surprise that, from Freud onward, emancipation tends to be figured in terms of greater capacities for love and work. [Italics in original]

### Alt Fails---2AC

#### The alt does absolutely nothing

Nik Hynek 13, Prof of International Relations and Theory of Politics at the Metropolitan University Prague and Charles University, with David Chandler, No emancipatory alternative, no critical security studies, Critical Studies on Security, 2013 Vol. 1, No. 1, 46–63, http://www.bristol.ac.uk/media-library/sites/spais/migrated/documents/cssrg1.pdf

[Note: CSS = “Critical Security Studies”]

These ‘post-emancipatory’ scholars still frame Western and international intervention in potentially emancipatory terms, but the horizons and aspirations have been substantially lowered from the universalist call to radical academic policy advocacy, of the founders of emancipatory approaches within security studies. While the initial confident calls for emancipatory alternatives at least had an understanding of the need for emancipatory agency, unfortunately found only in Western powers and international institutions, the later approaches lack this clarity and confidence, merely suggesting that more ‘open’, ‘unscripted’, ‘locally sensitive’, ‘desecuritised’ and less ‘universalist’ and ‘liberal’ approaches can avoid the ‘resistances’ held to come from the local level. If these approaches are ‘emancipatory’ they lack any clear project or programme as to what these claims might mean or how they might be carried out in reality and are little different to mainstream think tank proposals calling for more ‘local ownership’,

### Extinction Outweighs---2AC

#### Extinction outweighs---our framing shifts security policy from a national to existential frame---solves their threat K’s

Nathan Sears 20, PhD Candidate in Political Science at The University of Toronto and Trudeau Fellow in Peace, Conflict and Justice at the Munk School of Global Affairs, 4/17/20, “Existential Security: Towards a Security Framework for the Survival of Humanity,” https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.12800

Humanity’s capacity for self‐destruction poses a radically different problematique for security policy: survival interdependence . Survival interdependence means that the survival of human societies on one side of the world increasingly depends on the (in)action of human societies on the other. For most of history, human societies – clans, tribes, city‐states, empires, and nation states – could seek security irrespective of the security of other societies; but today no single nation state can solve the biggest security problems of the times on their own, nor in many cases can they hope to escape their security consequences. Humankind is becoming ever more tied together as a single ‘security unit’. The forces behind this process are not political – indeed, international politics remains stubbornly committed to ‘national security’ – but material (Deudney, 2007, 2018), especially certain human‐driven trends in technology and the environment that could threaten humanity with destruction. Security policy must take into account the significance of these changes. Thus, a new security framework is required.

‘Existential security’ responds to a similar set of questions as alternative security frames (see Table 2). Security for whom? The ‘referent object’ of existential security is humanity. Security is therefore about humanity’s survival . Security for which values? The ‘values’ to be secured are, at the minimum, the survival of humanity (i.e. the biological entity of the human species and cultural entity of human civilization), and, at the maximum, the long‐term prosperity of human civilization and the planet. The security of humankind ranges from the survival of existing human beings and societies to past and future generations of humanity – the past whose memory is recorded in history and preserved by the present, and the future whose possibilities of existence depend on actions taken in the present. Existential security therefore adopts an intergenerational perspective of security, not only for utilitarian reasons (e.g. quantifying the potential gains/losses in ‘future lives’) (Baum, 2015; Bostrom, 2002, 2013; Torres, 2017), but also because the significance of humankind – that is, all its past sufferings, present achievements, and future potential – is at stake, since existential risks simultaneously threaten humanity’s past, present, and future (Morgenthau, 1961).

How much security? Nick Bostrom (2013, p. 19) proposes the principle of ‘maxipok’, in which security policy would seek to ‘maximise the probability of an “OK outcome”, where an OK outcome is any outcome that avoids existential catastrophe’. While reducing the probability of existential risk to ‘zero’ may be impossible, the amount of security should be determined by a level of risk‐aversion equivalent to existential threats. Since thinking in terms of ‘worst‐case scenarios’ is a common practice in the security domain, and since some ‘worst‐case scenarios’ could include civilizational collapse or human extinction, this should imply a strong aversion to risk. Although there are logical limits to the ‘precautionary principle’ with respect to existential risks,10 it has practical implications for security policy, such as taking preventive, cost‐effective, and long‐term oriented action (Clarke, 2005). More generally, making (existential) security a priority does not imply the sacrifice of all other values (e.g. political liberty, economic wealth), but it does mean that potential gains in other values be weighed against potential losses in security. Security is always a question of degree (Wolfers, 1952).

From what threats? Existential security is concerned with those threats that have their origins in human agency and could bring about civilizational collapse or human extinction. This requires broadening the security agenda beyond its conventional focus on ‘security from violence’, while excluding ‘natural’ existential risks (e.g. asteroids and supervolcanos). There are two main reasons for emphasizing anthropogenic threats. The first is the low probability of natural risks on timescales relevant to humanity (Bostrom, 2013; Bostrom and Cirkovic, 2008;), whereas anthropogenic threats are, by definition, relevant to human timescales, including the twenty‐first century (Rees, 2003). The second is that many prevention/mitigation strategies for anthropogenic existential threats act on their drivers in human agency, which makes little sense for natural risks. The spectrum of anthropogenic existential threats includes threats to international peace and security (e.g. nuclear war), dangers from human intervention in the natural environment (e.g. climate change), and risks from emerging technologies (e.g. AI). Existential security must take into account the complex relationships between human, environmental, and technological systems, as well as inherent uncertainties about existential threat scenarios (e.g. ‘nuclear winter’, ‘hothouse Earth’, or ‘superintelligence’).

By what means and modes of protection? The existential security frame requires innovation in the means and modes of security policy. This is because the conventional emphasis on military capabilities and balancing is either inadequate (e.g. nuclear war), irrelevant (e.g. climate change), or counterproductive (e.g. AI). Moreover, the pursuit of relative gains/losses in security is fundamentally misguided for anthropogenic existential threats, since – as a general principle – either all human societies are safe, or none of them are. Existential security requires a paradigm shift from thinking about security policy as a matter of (national) ‘defense’ to being a matter of (global) ‘governance’. Governance is not an end in itself (e.g. the creation of a ‘world state’), but rather a means to security (i.e. the survival of humankind). The pursuit of existential security requires means of protection that involve a comprehensive set of political, economic, and technological resources – not merely military capabilities. The modes of protection are primarily ‘restraint’ and ‘resilience’. Restraint is a prevention strategy, while resilience is a mitigation strategy, which take on different forms for different threats. For the nuclear threat, restraint manifests itself in the policies of disarmament, arms control, and nonproliferation, while resilience comes mostly in the form of nuclear bunkers and shelters (Bull, 1961; Deudney, 2007). For climate change, restraint is primarily about limiting greenhouse gas emissions and the degradation of carbon sinks, while resilience is about making societies less vulnerable to heat stress, rising seas, food and water scarcities, new diseases, and human migration (Wallace‐Wells, 2019; World Bank, 2012). For AI, restraint entails the slow and careful development of AI (Bostrom, 2014) – or perhaps forgoing the ‘AI dream’ altogether (Joy, 2000) – while resilience is about reducing societal vulnerability to technological disruption (e.g. cybersecurity). Importantly, the growing survival interdependence of human societies implies that restraint and resilience must be mutual to be effective. If only some states choose disarmament or nonproliferation, if some societies reduce carbon emissions while others increase them, or if one technology firm decides to rapidly pursue ‘superintelligence’, then the (in)action of some actors may affect the security of all humankind. This emphasis on mutual restraint and resilience contrasts with the national security frame's emphasis on ‘self‐help’.

### Ontological Security Turn---2AC

#### Hybrid warfare disrupts NATO’s ontological security---reproduces the narrative of the “other” and turns the K---strengthening collective identity solves

Bahar Rumelili 15, Professor and Jean Monnet Chair at the Department of International Relations, Koc University, Istanbul, “Identity and desecuritisation: the pitfalls of conflating ontological and physical security,” Journal of International Relations and Development volume 18, pages52–74 (2015), https://link.springer.com/article/10.1057/jird.2013.22

With regard to ontological security, the distinction between security and insecurity is the more critical one. In a state of ontological insecurity, the Self experiences instability and uncertainty of being. Ontological insecurity refers to a state of disruption where the Self has lost its anchor for the definition of its identity and, consequently, its ability to sustain a narrative and answer questions about doing, acting, and being (Kinnvall 2004). It may arise from deep uncertainty (Mitzen 2006a) and/or from the failure to have its sense of Self affirmed by others (Zarakol 2010). Conversely, in a state of ontological security, the Self experiences a stable, certain, and consistent social existence, where it remains in control about its identity and capacity for action. While I do not rule out the possibility of a state of ontological asecurity, where the Self is simply not concerned with the stability and certainty of its identity, I do not explore this possibility and how it varies across different states of physical security in this article.

Having identified different states of physical and ontological security, I make the further assumption that since ontological and physical security are distinct, states of security do not vary uniformly across the ontological and physical layers of security. One can be at a state of physical insecurity while being at a state of ontological security, and vice versa. Consequently, Table 1 charts out the four possible states of security based on the conception of security as both ontological and physical.

The state of ontological insecurity/physical (in)security is one where the Self experiences concern about physical harm and the instability and uncertainty of its being. Ontological insecurity tempts actors to engage in practices that mark Others as not only different, but also as morally inferior and threatening (Campbell 1992). Ontological insecurity and physical (in)security reproduce one another. As actors seek ontologica l security through constructing Others as threats to their security-as-survival, they mobilise their physical defences in the pursuit of physical security through representing the sources of threat as different and morally inferior.

Similarly, in a state of ontological security/physical (in)security, actors experience stability and certainty of being in a relationship where the Other is constructed as threat to their security-as-survival. Consequently, they remain locked into conflict-producing routines to maintain their certainty of being (Mitzen 2006a). In protracted conflicts such as in Cyprus and Israel/Palestine, this state of security sustains a stable Self/Other relationship based on enemy roles. When in such a state of security, minority and majority groups, migrants and host societies perceive and represent each other’s identities as radically different and inherently incompatible, and reproduce these perceptions and representations through acts of securitisation in order to ensure their ontological security. The states of ontological insecurity/physical (in)security and ontological security/physical (in)security are both securitised states; however, whereas the former compels actors to construct new narratives of difference and threat and engage in the securitisation of new issues to regain their certainty and stability of being, the latter compels actors to reproduce the existing narratives and continue the securitisation of existing differences and conflicts to maintain it.

The state of ontological security/physical asecurity is certainly the most attractive state of security from a normative point of view. Security communities in international relations, and in particular, the European non-war community (Wæver 1998) and the Nordic community (Browning and Joenniemi 2012) constitute the best examples of such a state of security in international relations. A collective identity discourse makes it possible for states in security communities to maintain the us/them distinctions, which are necessary for the certainty and stability of being, while remaining in a state of physical asecurity vis-à-vis one another (Mitzen 2006b; Browning and Joenniemi 2012). In this state of security, conflicts are sustainably resolved; issues that have propelled conflict in the past are either settled or have shed their physical security-ness, and are negotiated in normal political channels. Yet, identity differences maintain their ontological security-ness as groups reproduce their distinct identities through various social and cultural practices.

### Ontological Security Turn---1AR

#### Hybrid warfare disrupts NATO’s ontological security---contingency planning solves by isolating NATO from existential fear

Maria Mälksoo 18, Senior Lecturer in International Security at the Brussels School of International Studies, University of Kent, “Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO,” European Security, 27:3, 374-392, https://dl1.cuni.cz/pluginfile.php/772169/mod\_resource/content/0/malksoo.pdf

Hybrid warfare indicates a multitude of possible contingencies, generating anxiety about one’s ability to remain oneself and to continue to act. It is thus linked to “anxiety over the vulnerability of [Western] power” (Bell 2012, pp. 230–231), threatening the West about losing its particularistic form of existence (cf. Creppell 2011, p. 455). Anxiety, in contrast to fear, which per Giddens (1991, p. 43) constitutes a response to a specific threat, concerns “perceived threats to the integrity of the security system of the individual” (Giddens 1991, pp. 44–45, cf. Browning and Joenniemi 2017, p. 38; Rumelili 2015). OS-seeking aims to mitigate the effects of such hard uncertainty, bringing it within bearable limits (Mitzen 2006, p. 346). Routines are instrumental here, as they “pacify the cognitive environment … ‘inoculating’ individuals against paralytic, deep fear of chaos” (Mitzen 2006, p. 347).

Being able to survive the “hybrid threats” is directly pertinent to the survival of the EU and NATO as particular kinds of organisations, underpinned and driven by specific values – which cannot be sacrificed or diluted in the struggle for physical and institutional survival. Yet, hybrid warfare disturbs the OS of the EU and NATO in subtly distinct ways. Due to the particularities of their institutional set-ups and historical foundations, the OS drives of the two organisations are somewhat distinctive. NATO’s history is occasionally told through its surpassing of a sequence of crises, albeit the end of the Cold War and the collapse of its original enemy created a situation of unprecedented uncertainty and ontological insecurity for the Alliance. Meanwhile, the EU’s ontological insecurity is a more recent phenomenon, stemming mostly from the Eurocrisis and the looming possibility of a Grexit a few years ago; the refugee/migration crisis in Europe of 2015 (Dingott Alkhoper 2018; Mitzen 2018); the actual UK decision on Brexit in 2016 (Browning 2018); and the rise of populist politics within the EU (Kinnvall, Manners, Mitzen 2018) and the United States. NATO as a military alliance has been historically more accustomed to the othering practices of concrete geographical places, whereas the EU is generally regarded as an organisation that has risen above geopolitical othering, juxtaposing itself to Europe’s dark past instead (Rumelili 2018, Subotic 2018, and Della Sala 2018). Accordingly, the EU might be more at home with hybrid threat management due to its historically broader conceptualisation of security through the paradigm of intertwined risks rather than being focused more strictly on “the threat, use and control of military force” in the manner of a traditional defence alliance (Walt 1991, p. 212; Manners 2002). Regardless of its perpetual transformer’s self-image, hybrid threats represent the uncomfortable “hard” or “fundamental” uncertainty for NATO (cf. Mitzen 2006, p. 346) and are thus ontologically disturbing for the security of its self as a traditional alliance with a collective security pledge bound to “armed attack” against one or more of its member states.

In order to achieve OS, actors strive for “routinizing their relations with significant others” (Mitzen 2006, p. 342). Routines help to keep ontological fears at bay, out of everyday discursive consciousness (Mitzen 2006, p. 348). From this perspective, NATO’s naming and shaming strategy vis-à-vis Russia as part of its hybrid warfare countering strategy links the uncertainty emanating from the hybrid nature of the new threats to the known and routine relationship with its traditional antagonist.8 The incapacitating difficulties related to planning ahead in anticipating and countering hybrid engagements are thus somewhat alleviated by the latter’s attachment to a known rival. Russia’s hybrid intervention in Ukraine has concurrently provided NATO with the familiar parameters of the cognitive “cocoon” (Giddens 1991, pp. 39–40) which enables the alliance to reproduce its cognitively “knowable” world. A Mitzenian reading of NATO’s emerging response to hybrid threats/warfare thus points at the renewed routinisation of the “programmed cognitive and behavioral responses” to Russia as the alliance’s original nemesis.

Restoring traditional vigilance vis-à-vis Russia, buttressing the forward defence along the Alliance’s eastern flank with the respective military reinforcements, contingency planning and exercises, the emerging response of NATO to the hybrid menace could also be read as an attempted restoration of a known normative order for the North Atlantic Alliance. Hybrid warfare endangers the basic features of the said normative order (or that of the broadly conceived Western security community in general, including the EU as well) as its efficient countering would likely compromise the underlying principles for this order’s particularistic existence (cf. Creppell 2011, p. 450). As a threat of subversion, hybrid warfare exposes the internal vulnerabilities in the body of the traditional security alliance (NATO) and a self-proclaimed post-modern security actor (i.e. the EU; cf. Cooper 2004). This concerns, in particular, the ever-elusive (and contested) balance between national/organisational security and individual liberties (cf. Waldron 2003, Neocleous 2007), as strategic communication is inherently at odds with free speech as a core value of Western liberalism. Countering hybrid warfare is conducive of generating a security predicament of perpetual pre-emption which, by definition, would indicate pre-emptive gathering of all sorts of data, thus likely infringing on the privacy of the individuals for the sake of the organisational/regional/national security. This precautionary logic resonates with the risk society approach which characterises the struggling with a sheer volume of risks with potentially fundamental consequences as a key feature of modernity, implying that “decisions are … made not in context of certainty, nor even of available knowledge, but of doubt, premonition, foreboding, challenge, mistrust, fear, and anxiety” (Ewald 2002, p. 294).

#### AND the ALT makes OS crisis worse

Filip Ejdus 19, Associate Professor of Security Studies at the Faculty of Political Sciences, University of Belgrade, “Crisis, Anxiety and Ontological Insecurity,” Crisis and Ontological Insecurity pp 7-37, 7/2/19, https://link.springer.com/chapter/10.1007/978-3-030-20667-3\_2

Critical Situations and Ontological Insecurity

The issue of critical situations which produce ontological insecurity of collective actors has been a neglected topic in the literature on OST in IR. So far, only a few authors have reflected on the role of critical situations in ontological security processes in world politics. Drawing on Giddens, Brent Steele for example argues that critical situations are unpredictable events that affect a large number of individuals, catch state agents off-guard and disrupt their self-identities (Steele 2008: 12). It is irrelevant, in his view, whether or not a researcher decides if an event constitutes a critical situation; what matters is whether policymakers interpret them as such. Critical situations are therefore not objective facts but social constructions produced in the very process of interpretation (ibid.). Dimitry Chernobrov has a similar understanding of international crises as unpredictable set of events that create great uncertainty and which states often (mis)recognise because they rely on narcissistic self-conceptions (Chernobrov 2016).

While I fully concur that critical situations are radical and socially constructed disruptions that put self-identities to the test, they seem to be more than that. In fact, such conceptualisation of a critical situation is so wide and elastic that most crises in world politics, if not all, can easily fit into this definition. For example, it could be argued that every terrorist attack is usually unpredictable, affects a large number of individuals, catches a state off-guard and disrupts self-identity narratives. And yet, if any crisis can be treated by analysts as a critical situation, the concept of ontological (in)security loses analytical sharpness and an important part of its value to IR theory. As a result of this conceptual underdevelopment, we currently have few conceptual tools in IR to identify and analyse critical situations and the conceptual distinction between ontological security and ontological insecurity remains elusive.

This book fills this gap by proposing a conceptual framework to study ontological insecurity and critical situations. By drawing on the work of Anthony Giddens, I define ontological security in world politics as possession, on the level of the unconscious and practical consciousness, of answers to four fundamental questions that all polities in some way need to address. These questions are related to existence; finitude; relations and auto-biography. Collective actors become ontologically insecure when critical situations rupture their routines, thus bringing fundamental questions to the level of discursive consciousness. Their inability to ‘bracket out’ fundamental questions produces anxiety and a loss of agency.

What does it mean to be ontologically secure? According to Giddens, ‘To be ontologically secure is to possess, on the level of the unconscious and practical consciousness, answers to fundamental existential questions which all human life in some way addresses’. These fundamental existential questions relate to existence and being, finitude and human life, the experience of others and the continuity of self-identity (Giddens 1991: 47). As he noted, ‘To live our lives we normally take for granted issues which, as centuries of philosophical enquiry have found, wither away under the sceptical gaze’ (Giddens 1991: 37). In other words, in order to be ontologically secure, agents have to be able to ‘bracket out’ these fundamental questions through routines of daily life, thus building trust into the constancy of their social and material environment and fending off existential anxieties. If unable to put aside these existential trepidations related to death, transience of life and the continuity of the self and others, individuals simply cannot ‘go on’ with their daily life. Ontological insecurity, on the other hand, is a result of critical situations, circumstances of radical and unpredictable disjuncture ‘that threaten or destroy the certitudes of institutionalised routines’ (Giddens 1984: 62). Critical situations remove the protective cocoon created by routines and move fundamental questions, previously taken for granted, into the realm of discursive consciousness. The result is the ‘flooding through’ of shame and guilt from the unconscious mind (ibid.: 57). The sudden inability of agents to ‘go on’ by relying on the unspoken know-how unleashes an upsurge of anxiety expressed in regressive modes of behaviour followed by attempts to re-establish routines and regain cognitive control over the changed environment (ibid.: 64). In these ‘faithful moments’ as Bahar Rumelili calls them, ‘anxieties can no longer be controlled’ and ‘ontological security comes under immediate strain’ (Rumelili 2015b: 11).

The distinction between discursive consciousness, practical consciousness and unconsciousness is of paramount importance here (Giddens 1984: 41–45). Discursive consciousness is the ability of actors to verbally express their actions. Practical consciousness, crucial for the maintenance of ontological security, is tacit knowledge about how to ‘go on’ without a need to express it discursively. Between practical and discursive consciousness there is a free flow of information. When asked to give discursive expression of something that is based on background knowledge, such as driving a car or practising table manners for example, agents are more or less able to do it but they do not need much knowledge to carry out a competent performance. Finally, unconsciousness includes cognitions that are ‘either wholly repressed from consciousness or appear in consciousness only in distorted form’ (ibid.: 5). Unlike practical and discursive consciousness, the unconscious mind is therefore separated from the previous two with a bar of repression.

The starting point of this book is that critical situations can also affect collective agents. However, in contrast to individual experience of anxiety that does not have to be expressed discursively, I posit that when collective actors are concerned, anxiety outbursts are performed through a public discourse on fundamental questions. Several studies on ontological security in IR have made a passing reference to this feature of ontological security as the ability to ‘bracket out’ fundamental questions in order to ‘go on’ with daily unfolding of international life (Kinnvall 2004: 759; Krolikowski 2008: 111; Steele 2008: 51). However, none of these studies have delved deeper into what these questions were, their relationship with critical situations and how all this could be translated into the field of world politics. In the rest of this section, I intend to bridge this gap. The first fundamental question is related to ‘existence and being’ that, according to Giddens, is about an ‘ontological framework of external reality’ (Giddens 1991: 48). This awareness ‘of being against non-being’ lies at the core of human freedom that generates anxiety. Giddens writes that answers to this fundamental question (like all others) are lodged at the level of practical consciousness. In pre-modern contexts, it was tradition that provided answers to this existential question and creates a sense of firmness of the world. In the context of high modernity, individuals can try to rely on tradition but this will not provide them with safe ground. Consequently, they have to continuously reflexively reorder their activities in light of new information.2

This book posits that collective actors in world politics also need to have trust in the continuity of their external environment. The society of states, with all its traditions and institutions, offers one such ontological framework for states (Bull 1977). To be ontologically secure in world politics, polities need to possess a practical understanding of what to expect from international society and build a sense of place in the existing order. To feel at home in international society is a precondition of states’ ontological security. The importance of home and dwelling to freedom from anxiety and ontological insecurity has been well documented in psychology and social theory (Dupuis and Thorns 1998; Padgett 2007). For individuals, home provides ‘a site of constancy in the social and material environment’ (Kinnvall 2004: 747). For polities, feeling at home in international society provides a sense of place in the international order and therefore a certain degree of cognitive control over their regional and international environment.

Bracketing out the fundamental questions is accomplished through routinisation of what the English School calls the primary institutions of international society. Here I have in mind ‘deep and relatively durable social practices’ such as diplomacy or international law that define legitimate behaviour and build the shared identity of states (Buzan 2014: 17). But the trust in durability of the secondary institutions of international society, such as security regimes or international organisations, can also inoculate states from existential anxieties. ‘States invest in international security institutions’, argue Berenskoetter and Giegerich, ‘because they enable states to gain (and sustain) ontological security by negotiating a shared sense of international order with friends’ (Berenskoetter and Giegerich 2010: 410). Taking part in these durable practices of international society provides constancy and thus helps contain—although falling short of fully overcoming—the chaos that is lurking below the surface of everyday unfolding of world politics.

Critical situations are generated by radical (real or perceived) ruptures in established routines of international society. As a result, the agent becomes disoriented, overwhelmed by ‘the anxiety of meaninglessness’ and ‘the loss of ultimate concern’ (Tillich 2000: 47; Rumelili 2015b: 12). Power transitions in the international system can engender ontological uncertainty even for the most powerful states that are fully integrated into the international society (Chacko 2014). However, states that are suspended in the outer tier of the society of states are much more vulnerable to ontological insecurity (Neumann 2010; Ejdus 2017). Even memories from past exclusion can provide fuel for the construction of critical situations. As Zarakol forcefully claimed, intersubjective pressures and stigmata exerted in the past by the ‘civilised’ society of states become with time an integral part of late entrants’ self-identity with significant consequences for their ontological (in)security (Zarakol 2010). ‘Rogue states’ such as North Korea, entirely ostracised from international society, face even greater intersubjective pressures. Ontologically vulnerable actors can try to routinise their subaltern position in the world through victimisation narratives and build their self-identity upon this feature. However, their anomic position and the relentless lack of trust in the world will occasionally fuel erratic outbursts of anxiety followed by defensive measures. These may wrongly appear to an outside observer as irrational behaviour, but they are in fact a form of ontological self-help.

### Perm---2AC

#### Perm do both---the alt fails, our securitization is good, no impact, and only the perm solves

Eric Van Rythoven 19. PhD in Political Science from Carleton University. Journal of Global Security Studies and the International Studies Association and the Canadian Political Science Association. “The Securitization Dilemma.” <https://academic.oup.com/jogss/advance-article/doi/10.1093/jogss/ogz028/5532523#137694797>.

Tragedy is largely absent from the existing normative debate on securitization. Instead, the debate has become organized around whether securitization is a “negative” or “positive” concept. In the classic formulation, the Copenhagen School points to how “[n]ational security should not be idealized. It works to silence opposition and has given power-holders many opportunities to exploit ‘threats’ for domestic purposes” (Buzan et al. 1998, 29; Williams 2003). Securitization has negative effects when it functions as “a political technology that consistently favors the interests of the powerful and enables violence and exclusion” (McDonald 2015, 154). Correspondingly, Wæver admits a “‘bias’ for desecuritization” or de-escalation, although he quickly notes that this is “not always better than securitization” (Wæver 2011, 469). At the same time, a number of approaches point to cases where securitization is ethically desirable. In her compelling consequentialist argument, for example, Floyd asks “whether the consequences of, and the gains from, the securitization are preferable relative to the consequences and gains from a politicization” (2007, 338). Relatedly, Roe contends that “the extent to which securitization necessitates a lack of openness and deliberation has been overexaggerated” and suggests it may even elicit unappreciated forms of cooperation (2012, 250).

The problem with the negative/positive debate is that it appears to impose moral certitude where there often is none. Registering securitizing moves as clearly positive or negative can be difficult because their effects can be mixed and temporally distant. The difficulty in making this determination may also be an indicator of the uncertainty surrounding securitizing moves. In the end, because the outcomes of security claims are uncertain, we cannot know in advance whether they will lead to positive or negative consequences. Instead, we should entertain a distinctly tragic vision of securitization that councils an ethic of self-limitation. The core of this tragic vision is a recognition that the powerful allure of using security talk to “gain control” over a situation will always be present (Wæver 1995, 54). However, we should also recognize that this control is always illusory because it presumes all of its effects can be predetermined. The tragedy of securitization is that the failure to recognize how contingency imposes limits on action lures political actors into a false sense of certainty and the conviction that they can determine the future. This leads to a hubristic adoption of “misplaced certainty,” such as when Vice President Dick Cheney declared in August of 2002 that “there is no doubt that Saddam Hussein now has weapons of mass destruction” (quoted in Mitzen and Schweller 2011, 3). A similar situation emerged when Secretary of Defense Donald Rumsfeld subsequently claimed in November that the Iraq conflict could be “[f]ive days or five weeks or five months, but it certainly isn’t going to last any longer than that” (Esterbrook 2002). A similarly misplaced certainty is evident in US General Stanley McChrystal’s assurances to the Obama administration in 2009 that a surge in troops and resources were critical to stave off American defeat in Afghanistan (Woodward 2009). More recently, it is visible in President Donald Trump’s 2018 assertion that he was “100 percent right” on the weaknesses of the Iran nuclear deal (CNN 2018).

Yet, tragedy cuts both ways. Blanket opposition to securitizing moves can also have unanticipated effects. Ironically, the desecuritization of an issue may not just result in its repoliticization, but in its disappearance from public view (Floyd 2010, 57–58). Viewing security discourse as negative also underplays how the management of threats can serve as a focal point for democratic cooperation among different political actors (Roe 2012, 250, 257–58). The point is not that every security discourse and the practices it justifies has catastrophically perverse consequences. Instead, the goal is to highlight a sensible restraint over the limits of seeing into the future, how this shapes choice, and the dangers of hubris that follow. When properly adapted to this constructivist context, the tragic vision of securitization can be an important tool in cultivating prudence and restraint (cf. Lebow 2003, 364).

The problem with this tragic vision is that it points to processes that are never entirely in our possession. Whether in the form of background knowledge (Pouliot 2008), habits (Hopf 2010), or routines (Mitzen 2006), much of social life occurs without conscious deliberation and reflection. These forms of unthinking action impair reflexivity and limit actors’ ability to see how the world might be different and thus how outcomes can be uncertain. In some cases, this can be benign, such as the unreflexive amity between Canada and the United States that allows these countries to “escape” from the traditional security dilemma (Collins 2014, 572–73). But just as practices of amity can be habitual, so too can enmity. The hawkish US senator may designate Iran’s nuclear program as threatening because that is what hawkish US senators do, and there is no perceived way to be hawkish otherwise. The result is that the uncertainty surrounding securitizing moves becomes concealed under an unthinking veil of common sense. The tragedy of securitization then is not only that political figures often exceed their limitations by ignoring how contingency can derail securitizing moves—it is that these limitations often never even register

This means overcoming the tragedy of securitization require a certain degree self-reflexivity. This is similar to what Booth and Wheeler describe as the “security dilemma sensibility,” or an actor’s ability and willingness to reflect upon their actions, including one’s own role in provoking insecurity in others (2008, 7). By sensitizing leaders to how uncertainty is an endemic feature of political life, and how their actions can be interpreted in unintended ways, security competition can be mitigated, at least in part (Booth and Wheeler 2008, 265). Yet, these moments of self-awareness and reflection are difficult precisely because there are powerful forces that demand simplicity and closure: namely our desire for a stable sense of self or what is widely referred to as ontological security (Mitzen 2006). Reflecting on the uncertainty of international politics can erode one’s sense of identity and agency, ultimately leading to a “deep, incapacitating state of not knowing how to get by in the world” (Mitzen and Schweller 2011, 29). Booth and Wheeler’s security dilemma sensibility may have the laudable goal of alerting leaders to the role of uncertainty in political life, but this confronts the problem that many would prefer that it remain hidden.

The consequence is that this tragic aspect of the securitization dilemma takes on an intractable character. Either unwilling or unable to “know one’s limits,” as Herz would say (1950, 179), the role of uncertainty becomes hidden and security claims appear as a reliable strategy for control and influence. Like the classic realist dilemma, the securitization dilemma is pervasive because it is often invisible. The compelling need for a logic of selflimitation—of a careful and reflective use of security language and how it can be derailed by contingency— is obscured because of an aversion to recognizinguncertainty. It is this specter of a need for reflection and restraint that may not be realized, I suggest, which demands that we rethink the role of the analyst in provoking reflexivity among power-holders.

Conclusion: Rethinking the Role of the Analyst

Motivated by the absence of unintended and perverse consequences in constructivist theorizing of security, this article has pursued a reconceptualization of the security dilemma. Viewing the dilemma as a logic of limitation shaped by choice, uncertainty, and tragedy, the argument focuses on transposing this logic to the constructivist context of securitization theory. By showing how the choice to engage in the social construction of threats is complicated by uncertainty and the tragic failure to recognize one’s own limits, the dilemma analytic helps us to understand how securitization can be both a potent instrument for mobilization, as well as a volatile source of unpredictability. Moreover, this conceptual lens lays the foundation for an ethical imperative of self-limitation among securitizing actors—albeit one made difficult given the desire for simplicity and closure. Far from a rebuke of constructivist theorizing, the argument shows that taking the social character of security seriously means appreciating how political claims are always vulnerable to being derailed by different types of contingency.

This reconstructive move has important implications for studying the social construction of security. First, while the initial influence of realism on securitization theory is well-documented (Floyd 2010; Gad and Peterson 2011), few attempts have been made to show how engaging with these realist roots can yield new insights.22 Here, the reconstruction of the security dilemma demonstrates how returning to realist themes can yield a fresh insights. Second, the argument pushes scholars studying securitization to expand their universe of outcomes beyond the reductive binary of success and failure and to consider cases of perverse and unintended consequences. Not only are these outcomes relatively common, they undercut the prevailing image of securitization as a reliable technology of control. Third, the securitization dilemma shows why uncertainty is more of an enduring problem for social action than constructivists typically acknowledge. Contra earlier arguments where learning and socialization effectively mitigate the problem of uncertainty (Wendt 2006, 208–9), this perspective stresses how contingency means that social acts like securitizing moves can have unpredictable effects.

The most important result of this reconstruction, however, may be in how taking the tragic element of the dilemma seriously reorders the political role of the analyst. Rather than assessing the validity of a particular security discourse, or exposing its socially constructed nature, this perspective asks the analyst to provoke reflexivity on behalf of power-holders over the risks associated with securitization. While this entails a bias toward deescalation and desecuritization, unlike other approaches this is not achieved through overt references to any liberal, democratic, or emancipatory ideal. Instead, it is packaged for power-holders as a strategy of self-preservation. Here, the analyst presents the move to securitize as a risk-laden and potentially self-defeating strategy. The analyst points to a series of precedents showing how such a strategy can produce perverse consequences: how today's tough talk can become tomorrow's liability; how audiences can interpret threatening messages in unexpected ways; and how today's framing of security can lead to perverse consequences tomorrow. By foregrounding the problem of uncertainty, the analyst works to accentuate and impress upon actors the dilemmatic quality of securitizing moves.

Yet, the problem with presenting the move to securitize as a risk is that it may become accepted. Ironically, framing an escalation in enmity as possible but dangerous is precisely what may legitimize such a move in the eyes of risk-insensitive actors. This is Huysmans’ (2002) now familiar normative dilemma of writing security. The indeterminacy of language means that political actors may interpret advice in unpredictable ways. Frustratingly, this may include the precise opposite of the analyst's intention. This situation is likely inescapable, but it may be mitigated. What I suggest is that analysts should strive to cultivate a deeper subjectivity of risk sensitivity, comparable to Booth and Wheeler's security-dilemma sensibility, among political actors.

Key to this argument is how visions of the future satisfy the human desire for certainty. As Berenskoetter argues, “visions depicting the self in an imagined future order serve as anxiety controlling mechanisms” (2011, 654). Visions of the future inoculate actors against the anxiety of uncertainty by providing a narrative of where they are going and how to get there. Indeed, normative debates on securitization are already loaded with such visions. The impulse to securitize is underpinned by a utopian future where the security frame can finally mobilize a response to an otherwise intractable problem. Conversely, the impulse to desecuritize is sustained by a dystopian future defined by unrestrained authoritarian politics. A tragic vision of the future does something different: it presents a future where the only thing we can know decisively is that it is indeterminate and attempts to conclusively control it are vulnerable to failure. The very recognition of fundamental limits on human freedom (Steele 2007, 281–82) becomes transformed into a source of ontological security. This tempers the human need for cognitive closure by reconfiguring it into what Herz understood as a “fundamentally humble posture toward the value and precariousness of life” (Sylvest 2008, 442). An actor with a greater sensitivity to indeterminacy may still pursue securitizing moves, but with a cautious awareness that they are volatile acts best pursued sparingly. The analyst does not simply educate political leaders by pointing to the indeterminacy of the world; she seeks to make political subjects more sensitive toward it by crafting visions of a precarious future.

Finally, this tragic vision cannot, and should not, escape its own need for reflexivity. Its scholarly proponents need to engage in their own process of self-reflection, focusing on how their knowledge and interests are themselves historically situated. The ethic of restraint is a value, and not necessarily the value for all historical circumstances. A recognition of the social construction of security “facts” must be sobered by a recognition of the social construction of security “values” (Hamati-Ataya 2012, 685).