# \*\*Neg\*\*

### EU CP

#### EU is key to solving Disinformation and is already Responding

Annina Claesson, April 8, 2019, "Coming Together to Fight Fake News: Lessons from the European Approach to Disinformation," CSIS, https://www.csis.org/coming-together-fight-fake-news-lessons-european-approach-disinformation

For observers across the pond, Europe has been a testing ground for tactics to counter disinformation in democracies**.** Over the course of many national elections in the past few years,Europe has tried a variety of measures to counter disinformation efforts from multiple sources**.** Now, the European Union is aiming to complement national efforts by scaling up its own response through EU-level policies**.**

In an effort to address what some civil society and media organizations have criticized as an overly disaggregated approach by the European Union, current EU efforts focus on proper coordination with and among the many actors involved in countering disinformation. Specifically, the EU response is focused on three lines of effort**:** improving interagency and international cooperation**; stepping up ambitions in addressing the role of the private sector;** and instituting a plan to support media literacy**.** In addition to helping the European Union tackle disinformation campaigns that seek to disrupt the democratic process, these measures can also serve as a template for the United States and other countries as they design their own anti-disinformation strategies.

Strengthening Interagency and International Cooperation

The problem of disinformation is a complex and disaggregated one. While the **United States often sees disinformation narrowly as the dissemination of “fake news” by Russian trolls**, the “European approach” often takes a wider view.1 its recent communications, the European Union presents disinformation as a problem rooted in complex and rapid socioeconomic changes. Our democracies are now characterized by stark societal divisions that malign actors may seek to exploit. While this is nothing new, technological developments have made disinformation a powerful, inexpensive, and often profitable method of influencing a range of actors from powerful states to small extremist groups. State-sponsored Russian campaigns in particular have become a mounting threat to European democracies and remain a significant challenge ahead of the 2019 European parliament elections, but other groups (such as those on the **far-right) have also been active in disinformation campaigns** in recent European elections.2,3

Since disinformation is a problem with diverse and complicated roots, the challenge of countering it does not land in any one portfolio. It requires cooperation between different agencies within states and internationally**.** As an important co-regulatory actor**,** this is where the European Union has a vital role to play. Over the course of 2018, the European Union has stepped up its ambitions in countering disinformation campaigns through a range of new initiatives.

#### EU for Nato support to counter disinformation:

Annina Claesson, April 8, 2019, "Coming Together to Fight Fake News: Lessons from the European Approach to Disinformation," CSIS, https://www.csis.org/coming-together-fight-fake-news-lessons-european-approach-disinformation

There are several positive lessons to draw from these. Perhaps most importantly, the **European Commission has appropriately identified the need for a unified,** multi-stakeholder response to disinformation**, including participation from governments, civil society, and the private sector**.4 The commission’s most recent action plan, released in December 2018, sets out important improvements in this regard. The EU budget for tackling disinformation is expected to more than double in 2019, going from €1.9 million in 2018 to €5 million.5 This is not to be disregarded—money matters a great deal, especially when Russia invests over €1 billion each year into their disinformation and propaganda efforts.6

The action plan’s most concrete new step is the creation of a rapid alert system, which provides alerts on new disinformation campaigns as they emerge in real time.7 This mechanism is set to involve NATO and could become a promising tool for intelligence and data sharing across borders**.** This action plan also strength- ens previously under-resourced tools such as the East Strategic Communication Task Force, an issue which was identified by experts as a significant roadblock to improving anti-disinformation efforts in the European Union.8

#### EU doesn’t even think we should take action against disinformation but is doing it anyaway.

Daniel Funke, 7-20-2022, "A guide to anti-misinformation actions around the world," Poynter, https://www.poynter.org/ifcn/anti-misinformation-actions/

BRUSSELS — In mid-March 2018, a European Commission high-level group published its final report on misinformation, drawing upon the input of experts from around the world who gathered over several weeks to help the European Union figure out what to do about misinformation. The report created by the high-level group — announced in November 2017 to help the EU craft policies to address growing concern about misinformation in Europe — contains an inclusive, collaborative approach to addressing misinformation around the world (Disclosure: Poynter attended the meetings as one of the experts). The report, while imperfect, explicitly recommends not regulating against misinformation — but the EU is only one of many governing bodies that have sought to stem the flow of online misinformation over the past few months. Spanning from Brazil to South Korea, these efforts raise questions about infringing free speech guarantees and are frequently victims of uncertainty. The muddying of the definition of fake news, the relative reach of which is still being studied, hinders governments’ ability to accomplish anything effective. In the spirit of this confusion, explained in detail in a Council of Europe report, Poynter has created a guide for existing attempts to legislate against what can broadly be referred to as online misinformation. While not every law contained here relates to misinformation specifically, they’ve all often been wrapped into that broader discussion. We have attempted to label different interventions as clearly as possible. Since these efforts seem to be announced weekly, this article will be updated on an ongoing basis.

### AT: Vaccines

#### Belief of scientific narratives of covid are high.

Agley, J., Xiao, Y., 1-7-2021, "Misinformation about COVID-19: evidence for differential latent profiles and a strong association with trust in science," BioMed Central, <https://bmcpublichealth.biomedcentral.com/articles/10.1186/s12889-020-10103-x>

For the full sample, believability of the narratives varied, from a low of 1.94 (SD=1.72) for the 5G narrative to a high of 5.56 (SD=1.64) for the zoonotic (scientific consensus) narrative. Four distinct belief profiles emerged, with the preponderance (70%) of the sample falling into Profile 1, which believed the scientifically accepted narrative (zoonotic origin) but not the misinformed or conspiratorial narratives. Other profiles did not disbelieve the zoonotic explanation, but rather believed additional misinformation to varying degrees. Controlling for sociodemographics, political orientation and religious commitment were marginally, and typically non-significantly, associated with COVID-19 belief profile membership. However, trust in science was a strong, significant predictor of profile membership, with lower trust being substantively associated with belonging to Profiles 2 through 4.

#### No link between misinformation and non-preventive disease behaviors.

Chan, HW., Chiu, C.PY., Zuo, S. et al., 5-4-2021, "Not-so-straightforward links between believing in COVID-19-related conspiracy theories and engaging in disease-preventive behaviours," Nature, https://www.nature.com/articles/s41599-021-00781-2#Sec16

Since the start of the COVID-19 pandemic, pertinent conspiracy theories have proliferated online, raising the question: How might believing in those conspiracy theories be linked with engagement in disease-preventive behaviours? To answer this, we conducted a repeated cross-sectional survey of around 1500 respondents to examine the link between conspiracy-theory beliefs and disease-preventive behaviours across six time-points in the United States from early February to late March 2020. The findings reveal that believing in risk-acceptance conspiracy theories (RA-CTs; e.g., “COVID-19 is a man-made bioweapon”) was linked to more preventive behaviours. However, believing in risk-rejection conspiracy theories (RR-CTs; e.g., “COVID-19 is like influenza and was purposefully exaggerated”) was associated with fewer preventive behaviours. These differential links were mediated by risk perception and negative emotions and modulated by the stage of the outbreak—RA-CTs predicted higher risk perception in the mild stage, whereas RR-CTs predicted lower risk perception in the severe stage.

#### People also opposed early disease preventative measures due to contradictions and lack of transparency from health organizations.

Lu He,21, 2021 Apr 24, "Why do people oppose mask wearing? A comprehensive analysis of U.S. tweets during the COVID-19 pandemic," PubMed Central (PMC), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7989302/

Further, some users opposed mask wearing because they believed that it was not an effective measure for preventing the spread of the virus and it was unnecessary for healthy individuals. These stances were indeed supported by authoritative bodies such as the CDC and the U.S. Surgeon General at the early stage of the pandemic. However, many of these tweets were posted in June and July, yet the CDC had reversed its position on public mask wearing in April. This finding indicates that certain segments of the U.S. population might not be aware of, or refuse to believe in, new recommendations from the CDC, and that earlier, contradicting recommendations might have a long-lasting impact. This means that public health experts and officials must clearly communicate about scientific uncertainty, reasons for specific recommendations, and the possibility that recommendations could change as more evidence emerges. In addition, public health experts should continue to engage the public so that new scientific findings, conclusions, and recommendations are immediately delivered to all members of the public.

#### Masking is high, reliance on misinformation is low, disease spreading was just natural.

Dennis Thompson, 10-22-2020, "Mask Use by Americans Now Tops 90%, Poll Finds," WebMD, <https://www.webmd.com/lung/news/20201022/mask-use-by-americans-now-tops-90-poll-finds#1>

More than nine in 10 U.S. adults (93%) said they sometimes, often or always wear a mask or face covering when they leave their home and are unable to socially distance, including more than seven in 10 (72%) who said they always do so, the poll revealed. "Compared to when we first asked this question in late August, our latest survey with HealthDay finds that more Americans are now consistently wearing a mask or face covering outside the home," said Kathy Steinberg, vice president of research for public release at The Harris Poll.

### AT: European Populism

#### **Populism declined drastically due to leaders’ mishandling of the pandemic and is unpopular in the squo – no democratic backsliding**

Bennett Institute of Public **P**olicy Cambridge 22 – The Bennett Institute of Public Policy is an organization at the University of Cambridge that researches public policy and politics. ("Support for populist politics ‘collapsed’ during the pandemic – global report," Bennett Institute for Public Policy, 1-18-2022, https://www.bennettinstitute.cam.ac.uk/blog/great-reset/, Accessed 7-20-2022, LASA-KS)

Support for populist parties and politicians, and agreement with populist sentiment, has diminished during the pandemic, according to a “mega-dataset” taking in attitudes of over half a million people across 109 countries since 2020. A University of Cambridge team say there are clear signs of a turning tide for the “populist wave”, as the mishandling of coronavirus by populist leaders – along with a desire for stability and a decline in “polarising” attitudes resulting from the pandemic – starts to move public opinion. The authors of the new report, from Cambridge’s Centre for the Future of Democracy (CFD), describe the study as the first global overview of how the Covid-19 crisis has affected political beliefs. They say that threats posed by the pandemic saw a “technocratic” shift in political authority worldwide, with increased trust in government, and in experts such as scientists and civil servants. Yet faith in the democratic process has continued to falter. “The story of politics in recent years has been the emergence of anti-establishment politicians who thrive on the growing distrust of experts,” said Dr Roberto Foa, Co-Director of the CFD and the report’s lead author. “From Erdogan and Bolsonaro to the ‘strong men’ of Eastern Europe, the planet has experienced a wave of political populism. Covid-19 may have caused that wave to crest.” “Electoral support for populist parties has collapsed around the world in a way we don’t see for more mainstream politicians. There is strong evidence that the pandemic has severely blunted the rise of populism,” said Foa. The findings are published today by Cambridge’s Bennett Institute for Public Policy. The first months of the pandemic saw many political leaders get a boost in ratings – a classic “rally round the flag” effect in troubled times, say researchers. However, the approval ratings of populist leaders the world over began declining almost as soon as coronavirus hit, and have continued to sink ever since. On average, populist leaders have seen a 10 percentage point drop between the spring of 2020 and the last quarter of 2021, while ratings for non-populists – on average – returned to around pre-pandemic levels. Electoral support also plunged for their parties – seen most clearly in Europe, where the proportion of people intending to vote for a populist party\* has fallen by an average of 11 percentage points to 27%. Overall, across Europe, early lockdowns saw voting intention for incumbent parties increase. Yet all the continent’s governing populists – from Italy’s Five Star to Hungary’s Fidezs – bucked the trend with the largest declines in support. Support for Europe’s opposition populist parties also fell over the pandemic – by 5 pp on average to 11% – while it rose for “mainstream” opposition. Researchers suggest several factors for populism’s fading appeal. One is simply the botch job made of the pandemic by populist governments: from Bolsonaro’s mask veto to Trump’s “bleach injection” suggestion. The report’s polling shows the public considered populist leaders to be less trustworthy sources of virus-related information than centrist counterparts. In June 2020, approval of government handling of the crisis was 11 percentage points lower on average in countries with populist leaders than in those with more centrist governance. By the end of 2020, this gap had widened to 16 points. Researchers also found that political “tribalism” – fertile ground for populists – has declined in most countries. The percentage of party supporters expressing a “strong dislike” of those who vote for opposing politicians fell in most nations (although not the US) during the crisis. “The pandemic fostered a sense of shared purpose that may have reduced the political polarisation we’ve seen over the last decade,” said CFD researcher and report co-author Dr Xavier Romero-Vidal. “This could help explain why populist leaders are struggling to mobilise support.” Some of the ideas propagated by populists are losing ground. Levels of agreement with statements such as “corrupt elites” divide our nation or the “will of the people” should be obeyed fell in almost every nation surveyed.

#### Populism is inevitable and a structural cause – drastic changes in social and economic affairs means misinformation is not key to its buildup in European politics – the aff won’t solve populism with the plan

Sheri Berman 19 – Berman teaches political science at Barnard College at Columbia University and writes scholarly articles of the political landscape of Europe. ("Populism is a Symptom Rather than a Cause: Democratic Disconnect, the Decline of the Center-Left, and the Rise of Populism in Western Europe," Polity, 9-26-2019, https://www.journals.uchicago.edu/doi/abs/10.1086/705378?journalCode=pol, Accessed 7-21-2022, LASA-KS)

How can we understand the rise of populism in Europe? Perhaps the most common approach is to look at the demand side, or the long-term structural changes that are said to have caused growing dissatisfaction with democracy and growing support for populism. This debate is primarily between those who stress economic factors and those who stress social factors. The former camp emphasizes the disruptive effects of globalization, neoliberalism, and technological change. In this view, increasing trade openness, the rise of non-Western economic powers, diminished government regulation, and growing automation have made life more insecure for the working and middle classes, have privileged highly educated and urban dwellers over less-educated and rural ones, and have made capitalism more of a zero-sum game.' These forces have also aggravated divisions within societies and between them. Over the past few decades, the economic winners have been the rising mid die classes in developing countries such as India and China and the wealthy in the West. The losers, meanwhile, have primarily been the lower and middle classes in the West, which explains their resentment of emerging economic powers as well as of elites in their own countries. The impact of these changes was exacerbated by the financial crisis of the late 2000s, which deepened social divisions and economic fears. A different narrative stresses social change as the root cause of populism. Over the past years, the foreign-born share of the population has reached historic heights in most European countries. The impact of this demographic shift was aggravated by the refugee crisis of 2015 and the fear generated by high-profile terrorist incidents, such as the November 2015 Islamist attacks in Paris, which killed over 400 people, and the December 2016 Islamist attack in Berlin that left a dozen people dead. The growth in the number of foreign-born residents, particularly of non-European backgrounds, occurred against the backdrop of an assault on traditional values that began the 1960s. According to this narrative, the cumulative impact of these change is that many citizens, particularly white males, have come to feel like strangers in their own countries. In this view, social change has led to a nativist or even racist backlash, with citizens growing dissatisfied with liberal democracy for allowing the decline of national cultures, traditions, and sovereignty. More recently, scholars have focused on the interaction between social and economic change. Ronald Inglehart and Pippa Norris argue that, during the postwar period, prosperity prompted a generational shift towards post-materialist values in the advanced industrial world that in turn prompted a reaction among more materialist voters. But this reaction exploded onto the political scene only when rising economic insecurity activated traditionalist and xenophobic attitudes that were already present. In a different analysis, Noam Gidron and Peter Hall stress the intraction of economic and social grievances, arguing that the decline of wellpaying, secure, respected jobs and the growing prominence and mobilization of women and minorities has combined to threaten the dominant status of white males in Western societies, leading to dissatisfaction with the political establishment and growing support for populist parties championing what they claim are"traditional" national identities and romanticizing an earlier status quo.' As real and as consequential as these economic and social changes have been, a focus on them alone can only reveal so much about the problems facing liberal democracy today. Populism is a symptom or reflection of growing dissatisfaction with democracy, and that dissatisfaction emerges when citizens believe that elites, parties, and governments are unwilling or unable to respond to their needs and demands. Change alone, in other words, is not destabilizing--it becomes so only if political institutions do not manage or mitigate it. To understand populism, inshort, one must examine how (or whether) elites, parties, and governments haven responded to the challenges that European societies have confronted over the last few decades. In democracies, unlike in dictatorships, when citizens become dissatisfied, they can express that dissatisfaction by voting to change their leaders and governments. But if citizens believe their votes do not matter-if their leaders and governments do not respond to their needs and demands--then their willingness to vote for parties critical of "the establishment" and of democracy more generally will grow.

#### Turn – Populism in opposition is good for democracy because it keeps the elite in check – no democratic backsliding in Europe, just a positive feedback loop to correct democracy

Jane Mansbridge and Stephen Macedo 20 – Mansbridge is the professor of political science Kennedy School of Government at Harvard University. She is one of the world’s most prominent scholars of democratic theory. Macedo is the Laurance S. Rockefeller Professor of Politics at Princeton University and he focuses on topics related to liberalism and democracy.("Populism and Democratic Theory,"Annual Review of Law and Social Science, 2-25-2020, https://www.princeton.edu/~macedo/Papers/Mansbridge%20Macedo%20Populism%20AnnRevLawSocSci%2019.pdf, Accessed 7-21-2022, LASA-KS)

Commentators routinely describe "populism" as vague. Some argue that the early US populists, who coined the modern usage, were not populists. We disagree and identify this common conceptual core: the "people" in a moral battle against "elites." The core definition fits all cases of populism: those on the left and right, those in the United States, Europe, and elsewhere. In addition to this minimal common core, we identify strongly suggested and frequently correlated non-core characteristics. These include the people's homogeneity and exclusivity, direct rule, and nationalism, as well as a single leader, vilification of vulnerable out-groups, and impatience with deliberation. The US Populist Party and Spain's Podemos Party fit the core definition but have few of the other characteristics. The core can be good for democracy, we argue, while the associated characteristics are often dangerous. Populism in opposition can be good for democracy, while populism in power carries great risks. We further distinguish, with many others (e.g., Judis 2016; Kazin 2017b; Mudde & Kaltwasser 2017; Müller 2016; Urbinati 2014, 2019a), between populism in opposition and populism in power. Populism in opposition often revitalizes democracy when the populist ideals and moral fervor anmating antagonism to entrenched elites crack through a prevailing political and discursive hegemony, bringing concerns that had been ignored or suppressed into the political arena. Yet populism in power poses risks to democracy. The same moral fervor and us/them dichotomy that help disrupt the entrenched political and cultural order when populists are in opposition militates against the mutual respect, tolerance, forbearance, negotiation, compromise, and respect for constitutional institutions necessary for egalitarian and pluralist democratic politics when populists take power. The core elements of populism are not antidemocratic. On the contrary, when a large group has designated itself "the people" and has come to see itself in a moral battle against "the elites," the members of that group have often had significant interests and values that political elites have neglected or even denigrated. At these moments, populism is democracy's way of saying, "Listen harder." Although ordinary citizens are not policy experts, they are in a position to judge how their lives are going, and when they have long-standing grievances that powerful elites have not effectively addressed, organizing in protest is a rationally and emotionally appropriate democratic response. Democracy particularly needs the populist impulse at certain historical moments. Elites often develop interests and values that diverge from those of the less affluent, less educated, and less privileged who live far from centers of political, economic, social, and cultural power. Thev often talk primarily with one another and reinforce one another. Power tends to beget more power. When groups with more power neglect the values and interests of the less powerful for too long, populism is what we want from democracy. the capacity to let the needs and values of the less powerful break through and thrust themselves on the increasingly insulated political, economic, social, and cultural ruling classes.

### AT: ISIS

#### ISIS not a threat---miniscule movements and impacts

Fareed Zakaria, 21, Zakaria is a columnist focusing on foreign affairs. He studied at Yale College and Harvard University, and is the host of CNN’s Fareed Zakaria GPS and contributing editor for the Atlantic; “**Ten years later, Islamist terrorism isn’t the threat it used to be**”, Washington Post, 4-29-2021, https://www.washingtonpost.com/opinions/global-opinions/ten-years-later-islamist-terrorism-isnt-the-threat-it-used-to-be/2021/04/29/deb88256-a91c-11eb-bca5-048b2759a489\_story.html/chuo

===says far-right terrorism is dangerous but if the impact’s just ISIS terrorism then we should be fine

This weekend marks the 10th anniversary of the operation, code-named Neptune Spear, that killed Osama bin Laden. It’s an opportunity to reflect on the state of Islamist terrorism and radical Islam more generally. And the initial diagnosis is clear: **The movement is in bad shape**. **Total deaths caused by terrorism around the world have plummeted by 59 percent since their peak in 2014.** In the West, the current threat is less from Islamist violence than far-right terrorism, which has surged by 250 percent in the same period, and now makes up 46 percent of attacks and 82 percent of deaths.

Most Islamist terrorism today tends to be **local** — the Taliban in Afghanistan, Boko Haram in Nigeria, al-Shabab in the Horn of Africa. That’s a major reversal from the glory days of al-Qaeda, when its leaders insisted that the focus must be not on the “near enemy” (the local regimes) but rather the “far enemy” (the United States and the West more broadly). Al-Qaeda has disintegrated into a bunch of militias in disparate places with no central command or ideology. The Islamic State is doing slightly better, with more funds, but it, too, **searches for unstable or ungoverned places**, such as Mozambique, where it can operate. **This focus on local conflicts erodes any global appeal.** Muslims around the world do not identify with local causes in Mozambique or Somalia.

Militant Islam, which began to flourish in the 1970s, rooted its appeal in failure — the failure of the dictatorships and monarchies of the Arab world to develop their societies. Islamists urged Muslims to give up on Western-style modernization, which had led only to poverty and tyranny, and to embrace instead the idea of political Islam — the road to an Islamic state. People such as bin Laden and his associate Ayman al-Zawahiri turned political Islam into militant Islam because they argued it was the only way to topple the dictatorships of the Arab world and beyond. They urged terrorism against those regimes but most importantly, against the superpower that supported them — the United States.

In an essay in the journal Religions, Nader Hashemi points out that the allure of political Islam was always that of an untested opposition movement, a mystical alternative to the shoddy reality that existed on the ground in the Muslim world. But over the past few decades, Islamist parties have entered the political process in Iraq, Sudan, Tunisia, Egypt, Gaza, Jordan and other places. “One general theme stands,” writes Hashemi. “The popular prestige of political Islam has been tarnished by its experience with state power.”

Millions of Muslims have now seen political Islam in action — and they don’t like it. They fled the Islamic State caliphate in droves. They protested against the Muslim Brotherhood in Egypt. They watched Shiite parties in Iraq turn into corrupt patronage operations. And in Iran, they continue to be deeply disenchanted by that country’s theocratic government. The oxygen that fed political Islam — disgust with the current regimes and blind faith in the promise of religious leaders — has been severely depleted.

**What remains now are local problems, local discontents that are really not part of some great global movement. It’s true in the West as well.** There has been a spate of Islamist attacks in France, but these were all carried out by individuals not previously known to the police and not part of any known jihadi groups. They were self-radicalized, with their own personal discomforts leading them to a radical ideology.

In this sense, Islamist attacks in Europe have something in common with far-right attacks in the United States. Alienated individuals, radicalizing online, find ideologies that weaponize their fears and furies. America has many more alienated White men these days than Muslims, hence the changing composition of the terrorism on its soil.

The lessons to draw about Islam, Islamist terrorism and the prospects for democracy in Islamic countries are complicated and varied. 2021 is also the 10th anniversary of the Arab Spring, when millions of Arabs tried to peacefully protest for democracy and human rights, a movement that sprouted up again over the past few years in Algeria, Sudan, Lebanon and Iraq. Though these efforts have had limited success, they show powerfully that Arabs and Muslims want freedom and democracy far more than they do a caliphate.

#### International deterrence, captures, and neutralization have eliminated the threat of ISIS

Orwa Ajjoub, 22, Ajjoub is a senior analyst at COAR global focusing on jihadism and Syria. He previously worked as an affiliated researcher at the Center for Middle Eastern Studies at Lund University; “ISIS has a new leader. It’s important to understand their operational capacity.”, Atlantic Council, 3-18-2022, https://www.atlanticcouncil.org/blogs/menasource/isis-has-a-new-leader-its-important-to-understand-their-operational-capacity-%EF%BF%BC/chuo

There are two types of jihad in the jihadi world that are determined by the reality on the ground and the jihadi groups’ capabilities: jihad al-tamkin, or jihad of empowerment, and jihad al-nikaya, or jihad of vexation and exhaustion. Under the former, the group seeks to control and rule over a geographical area and impose its interpretation of Islam. Under the latter, the goal is to inflict harm on the enemy’s interests with hit and run tactics suited to its lack of territory and manpower. Al-nikaya includes ambushes, suicide bombings, attacking prisons, and assassinations of leading enemy figures and collaborators. In 2014, when ISIS announced the establishment of its so-called caliphate, which stretched between eastern Syria and western Iraq, it shifted from jihad al-nikaya to jihad al-tamkin. However, with its loss of territories and assets, which started in 2016, the group has gradually but systematically returned to jihad al-nikaya.

While al-Qaeda has been largely loyal to al-nikaya—as evidenced by the September 11, 2001 terrorist attacks as well as the 2004 Madrid and 2005 London bombings—claiming that it wasn’t yet time to announce the establishment of the caliphate, ISIS hasn’t only alternated between the two based on the reality on the ground but also merged during its heyday between 2010 and 2014, as noted by scholar Hassan Abu Hannyia.

ISIS’s attempt to free its fighters from prisons isn’t new and **reflects the group’s increased need for manpower**. In November 2021, the SDF and US-led international coalition thwarted a plot by a suspected ISIS cell in eastern Deir ez-Zor province, which was planning to attack the same prison. **The group’s manpower has significantly diminished since its territorial defeat in 2019. Thousands of attacks in Syria and Iraq has worn ISIS down, as well as its enemies’ ability to neutralize or capture thousands of its fighters.**

According to Jihad Analytics, a consultancy company on global and cyber jihad, ISIS claimed 1,764 and 3,144 attacks in Syria and Iraq, respectively, between March 2019 and January 2022. While a 2019 United Nations (UN) report estimated that ISIS had up to eighteen thousand fighters, including three thousand foreign fighters operating in Syria and Iraq, **a recent 2022 UN assessment claims that the group has only retained between six thousand and ten thousand, which means that ISIS has lost almost half of its fighters via death or capture.** Today, the SDF still holds ten thousand ISIS fighters in its prisons, which is seen as a valuable pool for the **group’s drained rank and file**. This was reflected by two speeches made by ISIS spokesman, Abu Hamza al-Qurashi, in June and October 2021, in which he explicitly called his supporters to free ISIS inmates from SDF prisons.

**The international war against ISIS has deprived the group of the territories it once controlled and clamped down on regional borders, closing the pipeline of foreign fighters coming into Syria, most of whom are known for their ideological intransigence and fighting experiences.** This reality has pushed the group to rely more on local fighters, who don’t necessarily believe in its ideology but, rather, were pushed by local grievances generated by social inequality, political exclusion, and a lack of better options.

#### ISIS has no capabilities to attack

David Sterman, 19, Sterman is a senior policy analyst at the international security program, he holds a master’s degree from Georgetown’s Center of Security Studies. His current research focuses on terrorism and violent extremism in America, immigration and terrorist threats, foreign fighter recruitment, and the effectiveness and consequences of American counterterrorism efforts; “Decision-Making in the Counter-ISIS War”, New America, 11-15-2019, https://www.newamerica.org/international-security/reports/decision-making-counter-isis-war/appendix/chuo

===uhh not the best card

One of the clearest signs that the **ISIS threat was not imminent** at the time the counter-ISIS war was initiated is that the government itself repeatedly and via various institutions assessed that there was no known evidence of a direct ISIS threat to the homeland. The government continued to share this assessment long after the decision to initiate the counter-ISIS war was made, suggesting that it did not view its initial assessment as incorrect.

Among those who made such comments are President Obama himself, who on September 10, while authorizing the escalation of the war into Syria stated that “we have not yet detected specific plotting against our homeland.”162 National Counterterrorism Center Director Matt Olsen said that “we have no credible information that ISIL is planning to attack the United States” and described the threat as potential, adding there was no evidence of ISIS cell development inside the United States.163 Also in September, Department of Homeland Security Secretary Jeh Johnson stated, “At present, we have no credible information that [ISIS] is planning to attack the homeland of the United States.”164 In August 2014, Pentagon Spokesperson Rear Admiral John Kirby stated that the Defense Department did not believe that ISIS had “the capability right now to conduct a major attack on the U.S. homeland.”165 Chairman of the Joint Chiefs of Staff General Martin Dempsey also stated in August that there had not yet been evidence that ISIS was engaged in “active plotting against the homeland, so it’s different than that which we see in Yemen.”166 Nor did officials change their assessment with the beginning of the military campaign. In February 2015, Department of Homeland Security Undersecretary for the Office of Intelligence and Analysis Francis X. Taylor said, “We are unaware of any specific, credible, imminent threat to the Homeland.”167

The Department of Homeland Security’s National Terrorism Advisory System (NTAS) provides another set of evidence of the government’s lack of knowledge of any direct ISIS threat to the homeland. In April 2011, the Department of Homeland Security replaced the infamous color-coded Homeland Security Advisory system with NTAS. Under the NTAS system, an alert would be sent out when there was important information distinguishing between either an “elevated” threat with no specific information on timing or location or an “imminent” threat otherwise.168 Even as ISIS spread across Iraq and the United States initiated its counter-ISIS war in 2014, NTAS provided no alerts until December 2015, when it issued its first bulletin.169

The first bulletin, released on December 16, 2015, read, “We know of no intelligence that is both specific and credible at this time of a plot by terrorist organizations to attack the homeland.”170 The first bulletin was replaced by a second bulletin issued on June 15, 2016 that stated the previous bulletin’s “basic assessment has not changed.”171 In the wake of the deadly ISIS-inspired attack in Orlando, the bulletin again repeated that “we know of no intelligence that is both specific and credible at this time of a plot by terrorist organizations to attack the homeland” while reiterating the threat of inspired violence, which was also described in the previous bulletin.172

One of the clearest signs that the ISIS threat was not imminent is that the government **repeatedly** and via various institutions assessed that there was no known evidence of a direct ISIS threat to the homeland.

In November 2016 a new bulletin again reported no change in the basic assessment, emphasized inspired violence, and reiterated the lack of evidence of credible plots to attack the homeland by foreign terrorist organizations.173

However, it seems unlikely that this change represented newfound organizational plots against the United States. **The bulk of the bulletin remains focused on inspired and enabled violence, no alert was provided regarding an imminent threat, and the bulletin came as ISIS's territorial holdings crumbled.**

Another set of sources for evaluating the government’s assessment of the ISIS threat to the homeland is the U.S. intelligence community’s Worldwide Threat Assessments. These assessments repeatedly stated that the most likely threat to the United States remained homegrown terrorism rather than ISIS-directed attacks.177 Though none of these assessments include language denying foreign terrorist organization plots, it would be odd if there was a major credible threat and the assessments failed to mention it while emphasizing homegrown, inspired violence.

Government statements are limited in their ability to measure whether there is in fact a direct threat. They can be incorrect in their assessments or the threat can grow rapidly after an assessment is made.178 It is therefore important to also look at the indicators themselves.

The primary indicator of threat referenced in justifying the need for military action to respond to growing risks to the homeland was the large number of foreign fighters traveling to Syria and Iraq.179 Other oft-cited indicators included the extent of territory and money available to ISIS, which could allow it to be selective in recruiting for and preparing sophisticated elite-staffed attack plots from its safe haven and its ability to launch multiple attack plots without needing each one to succeed.180 These indicators are very real sources of concern, yet they **do not constitute evidence of a direct threat that would turn America’s preventive logic into a preemptive logic**.

There is a geographic split in the indicators. The above indicators of threat exist on the Syria and Iraq side of the ledger, describing how ISIS managed to build an unprecedented safe haven that could potentially pose a risk to the homeland and absolutely posed a threat to those living in or near ISIS's territory. In contrast, viewed from the United States’ side, the indicators did not show a substantial threat to the homeland. In the 18 years since 9/11, no jihadist foreign terrorist organization has carried out a deadly attack inside the United States and no foreign fighter or individual who received terrorist training181 abroad has carried out a deadly attack, according to New America’s research.182

ISIS's rise sparked fears that the United States’ record of success in avoiding attacks might change. **Yet more than five years after the United States’ initiation of a counterterrorism war, and eight years into the Syrian conflict, there is little evidence that ISIS developed the capability to direct attacks inside the United States.** Of course, it is possible that, absent intervention, ISIS would have developed the capability, but that is a preventive logic. **If ISIS had the capability prior to the initiation of the war, it would be expected that there would be some evidence of that capability’s development by now.**

More than five years after the United States’ initiation of a counterterrorism war, and eight years into the Syrian conflict, **there is little evidence ISIS developed the capability to direct attacks inside the United States**.

The number of Americans who joined ISIS or otherwise traveled to fight in Syria was relatively low compared to other countries. In August 2014, the government placed the number of Americans fighting with any faction in Syria at 100 people, and National Counterterrorism Center Director Matthew Olsen confirmed that the number fighting with ISIS was likely about a dozen individuals.188 The United States’ latest updated count is that 300 Americans went or attempted to fight with any group in Syria.189

Far from discussing an influx of returnees to the United States, Olsen portrayed it as a matter of individuals returning.190 Public tracking of known returnees has identified relatively few who returned to the United States, many of whom came back under the supervision of law enforcement.191 Whatever the true number, it is far from the feared wave of returnees.

While many pointed to the Afghan conflict as an example of the danger of foreign fighter flows, in the more recent foreign fighter mobilization to Somalia, no returnee to the United States was accused of plotting an attack.192 It is reasonable to suggest that ISIS was a different type of organization with more power and thus posed a greater threat of attacks on the homeland than al Shabaab.193 On the other hand, it is worth noting that prior to 9/11, the United States did very little to track jihadist foreign fighters, making the Afghanistan case a questionable comparison for post-9/11 threat assessments.194

The amount in question in the Elshinawy case is small and not dissimilar from what ISIS sympathizers are able to raise via means of self-financing.200 Four men were able to raise that amount of funds in a case based out of San Diego to send to al Shabaab in 2007 and 2008.201 In addition, the threat was not dependent on ISIS's territory in Syria, and could be more effective when conducted from outside of Syria in a dispersed network of the kind likely to be left after military action.202 The Elshinawy case provides a warning regarding jihadist innovations, but it does not demonstrate a great capability of ISIS to finance terror inside the United States.

### AT: China

#### \*\*\* The NATO bad Russia- China alliance links well to this aff

#### China won’t invade Taiwan any time soon and they aren’t trying to distract the US

Tirpak 5-11-22 Tirpak , John. A. (2022, May 11). Top intel: China not ready to invade Taiwan; Ukraine War in stalemate. Air Force Magazine. Retrieved July 21, 2022, from https://www.airforcemag.com/top-intel-china-not-ready-to-invade-taiwan-ukraine-war-in-stalemate/ John A. Tirpak is Editorial Director of Air Force Magazine. He has been recognized with awards for journalistic excellence from the Society of Professional Journalists, the Aviation and Space Writer’s Association, the Association of Business Publications International, and was the recipient of the 2018 Gill Robb Wilson Award in Arts and Letters from the Air Force Association.

**China isn’t** yet **prepared to successfully invade Taiwan and** probably **won’t try it soon in the belief that the U.S. is “distracted” by the Ukraine war**, said Avril Haines, Director of National Intelligence, during a Senate Armed Services Committee hearing. She also said that while there’s no clear end in sight to Russia’s invasion, the Intelligence Community doubts Russia will quit, but also doubts Russia will resort to nuclear weapons in the near future. Senators lauded the Intelligence Community for correctly predicting the Ukraine war, but criticized it for its failure to predict Ukraine’s success in resisting the invasion and Russia’s troubles in carrying it out. “Thus far, the **IC does not assess that the Russia-Ukraine crisis is likely to accelerate [China’s] plan vis-a-vis Taiwan**,” Haines said on May 10. China was “surprised by the degree to which the United States and Europe came together to enact sanctions, and that is something they obviously will be looking at in the context of Taiwan,” Haines said. Also, “one of the issues for them is the confidence they have that they are able to take action in Taiwan over our intervention.” This will “play into their decision-making over time.” Seeing events unfold in Ukraine “may give them less confidence, in some respects, over what is likely to happen” in a Taiwan invasion, Haines said. Haines and Defense Intelligence Agency chief Lt. Gen. Scott D. Berrier said 2027 is the point at which the U.S. thinks China believes it could prevail over a U.S. intervention to pull off a successful Taiwan invasion, noting China may therefore accelerate that date. They also said Taiwan needs to do more to prepare to defend itself, both in equipment and the structure of its military.

### AT: Iran Cyber

#### No motive---they keep it small to avoid escalation

Dr. James Andrew Lewis 18, Senior Vice President at the Center for Strategic and International Studies, Ph.D. from the University of Chicago, January 2018, “Rethinking Cybersecurity: Strategy, Mass Effect, and States,” <https://tinyurl.com/y27xcqbb>, p. 7-11

The Russians specialize in coercion, financial crime, and creating harmful cognitive effect—the ability to manipulate emotions and decisionmaking. Under their 2010 military doctrine on disruptive information operations (part of what they call "New Generation Warfare"). Russians want confusion, not physical damage. Iran and North Korea use cyber actions against American banks or entertainment companies like Sony or the Sands Casino, but their goal is political coercion, not destruction.

None of these countries talk about death by 1000 cuts or attacking critical infrastructure to produce a cyber Pearl Harbor or any of the other scenarios that dominate the media. The few disruptive attacks on critical infrastructure have focused almost exclusively on the energy sector. Major financial institutions face a high degree of risk but in most cases, the attackers' intent is to extract money. There have been cases of service disruption and data erasure, but these have been limited in scope. Denial-of-service attacks against banks impede services and may be costly to the targeted bank, but do not have a major effect on the national economy. In all of these actions, there is a line that countries have been unwilling to cross.

When our opponents decided to challenge American "hegemony," they developed strategies to circumvent the risks of retaliation or escalation by ensuring that their actions stayed below the use-of-force threshold—an imprecise threshold, roughly defined by international law, but usually considered to involve actions that produce destruction or casualties. Almost all cyber attacks fall below this threshold, including, crime, espionage, and politically coercive acts. This explains why the decades-long quest to rebuild Cold War deterrence in cyberspace has been fruitless.

It also explains why we have not seen the dreaded cyber Pearl Harbor or other predicted catastrophes. Opponents are keenly aware that launching catastrophe brings with it immense risk of receiving catastrophe in return. States are the only actors who can carry out catastrophic cyber attacks and they are very unlikely to do so in a strategic environment that seeks to gain advantage without engaging in armed conflict. Decisions on targets and attack make sense only when embedded in their larger strategic calculations regarding how best to fight with the United States.

#### Iran avoids escalation and focuses on using lobbying instead

Ali **Hajizade**, 20 May ,2020, "Iran’s selective approach to hybrid war," Al Arabiya English, https://english.alarabiya.net/views/news/middle-east/2018/02/23/Iran-s-selective-approach-to-hybrid-war

During the cold war, the world witnessed various proxy wars, involving USSR and the USA, and their official and unofficial allies. Moscow and Washington managed to wage proxy wars in Vietnam, Angola, Afghanistan and other parts of the world.

Now there is no Warsaw block, and proxy wars could seemingly become history. However, it did not happen. In today’s world, certain regional players have adopted the Soviet method of waging proxy wars. Speaking of the Middle East, we should emphasize Iran’s activity.

Strategists from Tehran are to be lauded; they improved the Soviet methods and transformed them into a system of a comprehensive hybrid war, including the application of modern technologies. Today, Iran’s permanent hybrid war is mainly directed against three countries – USA, Israel and Saudi Arabia. However, Tehran is selective about the approach to each of these countries.

Iran has a separate strategy for each of these countries. However, in each case Iran tries to avoid a straightforward confrontation. For example, the situation with US is much more nuanced than with Israel or Saudi Arabia.

For instance, Iranian authorities declare vicious slogans against “Great Satan”, but at the same time, they spend great financial resources and energy to create, expand and support Iranian Lobby in US. These efforts continued even when Iran, not directly, but through Shiite armed militias was involved in a military conflict with the US army in Iraq. Iranians have been contacting with representatives of the Iraqi opposition since Saddam Hussein’s years in power.

The American invasion freed Iran’s hands and Tehran was able to fully use its ties and influence over Shiites in Iraq. Thus, Iraq turned into a failed state, possessing a role of a buffer zone for Iran.

They could establish very valuable ties with a certain part (mainly with the liberal wing) of the American and European political establishment through the work of Iranian Lobby in US and EU.

Ethnic Iranians including Iranians who have dual citizenship participate in the work of Iranian Lobby together with citizens of Western countries, among which there are politicians, social activists, experts and journalists. The Head of Iran’s intelligence Mahmoud Alavi explicitly stated this in the interview.

The main objective of Iranian Lobby in Washington is to counteract activities of Jewish Lobby and activities of Israel, Saudi Arabia and UAE in Washington. In particular, in matters regarding Iran, for example Iranian nuclear program, Iran’s missile program, matters related to tightening of sanctions against Iran and Iran’s ties with terrorist organizations.

#### Cyber attacks are not severe and countries sought to avoid violent conflicts

Jason **Healey**, 3-9-20**22**, "Preventing Cyber Escalation in Ukraine and After," War on the Rocks, https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/

So far, cyber attacks have not proven particularly escalatory or effective on the battlefield. Even the most provocative incidents that came closest to resembling kinetic attacks, such as Stuxnet or the ransomware attack on Colonial Pipeline, have not led to particularly menacing crises, much less war. If anything, over the past decade cyber capabilities have helped de-escalate crises, acting as a “non-kinetic option for leaders who feel pressure to act in a crisis, but who are wary of using force.”

The U.S. conflict with Iran offers a clear example. After Iran attacked several oil tankers and downed a U.S. drone in June 2019, President Donald Trump canceled punitive U.S. airstrikes at the last minute out of concern that the casualties could prompt further escalation. However, he allowed nonlethal cyber disruption of Iranian computer systems, anticipating Iran would not respond violently. Indeed, Iran’s supreme leader “blocked any large, direct retaliation,” limiting the country’s response to the cyber realm.

Scholars have offered different explanations for the non-escalatory nature of these attacks. Cyber effects are “uncertain and often relatively limited” and “offer great powers escalatory offramps [and] signaling mechanisms” to de-escalate. In the “cyber strategic competitive space short of armed conflict,” states have “tacitly agreed on lower and upper bounds” and accordingly “have mutual interests in avoiding escalation to violent conflict.” Cyber conflict also has characteristics of an intelligence, not military, contest.

#### Russia’s invasion on Ukraine has undermined cohesion in NATO and EU countries due to disagreements on sanctions

Luigi **Scazzieri**, 6-15-20**22**, "Have we passed the high-water mark of European unity on Ukraine?," EUROPP, <https://blogs.lse.ac.uk/europpblog/2022/06/15/have-we-passed-the-high-water-mark-of-european-unity-on-ukraine/>

EU leaders presented a united response in the immediate aftermath of Russia’s invasion of Ukraine. Yet as the war continues, th**is unity is coming under strain**. Luigi Scazzieri argues there is now a real risk that rifts sparked by the conflict could become entrenched, undermining European cohesion on issues far beyond the war in Ukraine.

When Vladimir Putin launched his invasion of Ukraine in February this year, EU leaders quickly agreed to impose sweeping sanctions on Russia’s economy and to provide Kyiv with military and financial assistance. But as the conflict enters a new phase, European unity is coming under strain.

At the start of the war, a Russian victory seemed likely. But Ukraine managed to halt the Russian assault on Kyiv, forcing Moscow to focus on the Donbas and Ukraine’s south. Even here, Russia’s offensive appears to have limited momentum. Russia has suffered extensive losses and will struggle to carry out large-scale offensive operations. At the same time, Ukrainian forces will find it harder to retake territory than they did to defend it. Both sides will struggle to achieve a breakthrough.

As the conflict continues, splits between European countries will deepen. **Divisions over increasing sanctions on Russia are already highly visible.**It was difficult for the EU to agree on the sixth package of sanctions at the end of May, especially on Russian oil imports. To overcome Hungary’s opposition, EU leaders had to agree not to sanction imports via pipeline. It will be even more challenging for the EU to sanction Russian gas, as member states like Germany, Austria, and Hungary, which are highly dependent on Russian gas, fear they could not cope with a complete cut-off. This will increase tensions with those member states who argue that gas revenues are essential in fueling Russia’s war effort.

Rifts over strategy are also becoming highly apparent. Eastern EU member states, particularly Poland and the Baltic states, fear they may be invaded next if Ukraine loses and are convinced of the need to provide Kyiv with extensive support to help it prevail. They also think that negotiations with Russia are pointless, as Putin cannot be trusted to implement any agreement. Conversely, while western EU states like France, Germany and Italy have provided ample support to Ukraine, they think the conflict should end through a negotiation between Russia and Ukraine, potentially involving some compromises by Kyiv. Western EU countries don’t believe there is a risk that Russia could attack NATO countries, but instead worry about the risk of the conflict escalating into a NATO-Russia one.

This western European attitude sparks fears in the hawkish eastern states that western Europeans are willing to appease Putin and that they underestimate the threat from Russia. These fears have been compounded by Germany’s delays in delivering weapons to Ukraine. Similarly, French President Emmanuel Macron’s references to the need to avoid humiliating Russia are seen as signals that he is willing to push Ukraine to make concessions to Russia, even though he denies this. France, Germany and Italy have all called for a ceasefire, causing tensions with eastern member states, who think this would entrench Russian control over parts of Ukraine.

The battle of attrition in the Donbas may eventually persuade Russia and Ukraine to agree to a ceasefire. But this could deepen European differences further. If Russia’s advance forced Ukraine to accept territorial losses as part of an agreement, most EU countries would favour maintaining the bulk of sanctions to avoid legitimising Putin’s gains. But over time, calls could grow for sanctions to be eased, deepening divisions.

Conversely, if Ukrainian advances persuaded Putin that it was in his interest to withdraw from the territories occupied since February, this could be even more divisive. The hawkish EU states would want to maintain the sanctions and would reject any attempt to normalise relations with Russia for as long as Putin was in power. Meanwhile, the dovish countries would likely favour lifting some sanctions and would try to rebuild a more stable relationship with Moscow, for example focusing on arms control talks.

**The biggest European divisions would occur if Ukraine was extremely successful in retaking territory.** Putin may accept losing the territories that Russia has occupied since February, and perhaps even those parts of the Donbas that Russia has controlled since 2014. But neither Putin, nor any potential successor, could easily accept losing Crimea. If faced with such a possibility, Russia would double down on the war, and the risk of Putin being willing to use nuclear weapons to force Kyiv to back down would also rise. As CIA Director Bill Burns recently highlighted in an interview, Putin “doesn’t believe he can afford to lose”. Most EU countries would not be comfortable with such a risky escalation, but some might insist that Putin is bluffing.

Three months after Russia’s invasion, Kyiv’s resistance has ensured that Russia has not achieved its original aim of subjugating Ukraine, but the war’s outcome remains unclear. What is certain is that the conflict is breeding mistrust amongst EU states and that divisions are likely to deepen further. The risk is that the rifts sparked by the conflict could become entrenched, undermining European cohesion on issues well beyond the war in Ukraine and policy towards Russia.

#### There are more pressing issues in the relationship to worry about than North Korea cyber

“North Korea's Offensive Cyber Program Might Be Good, but Is It Effective?” Council on Foreign Relations, **Council on Foreign Relations**, https://www.cfr.org/blog/north-koreas-offensive-cyber-program-might-be-good-it-effective. 10/25/20**17**

**North Korea uses cyber strategies**, as it does nuclear posture and ballistic missile tests, to signal resolve and capability in its ongoing crisis with South Korea and the United States. **Yet, no** North Korea cyber **operation has caused a government to back down.** Last week in Net Politics, Erica Borghard argued that U.S. signals to North Korea are not sufficiently coercive to compel Pyongyang to change course. So why don’t experts treat North Korea’s cyber-based signals with the same amount of moderation? Most of North Korea’s cyber actions occur against either South Korea or the United States, usually low-level website defacements or DDoS signaling campaigns that do not escalate. Between 2000 and 2014, we count a total of 16 cyber operations launched against North Korea’s rivals. Exactly **zero** of these **operations are coercive successes against opposition** governments. **North Korea has** lots of potential but **little** actual demonstrated **ability to achieve** leverage **through cyber operations.** They might prove the world wrong at some point, as they have on the nuclear front, but **there are more pressing issues** in the relationship **to worry** about **than North Korea’s ability to achieve coercion in cyberspace.**

### AT: North Korean Cyber

#### No hybrid war

Dr. Samuel Charap 16, Ph.D. in Political Science from the University of Oxford, M.Phil. in Russian and East European Studies from the University of Oxford, B.A. in Political Science and Russian from Amherst College, Senior Fellow for Russia and Eurasia at the International Institute for Strategic Studies, “The Ghost of Hybrid War”, Survival, Volume 57, Number 6, December 2015 – January 2016

Analysts in the West tend to think that Russia would choose hybrid tactics in order to sow discord within NATO – using ambiguity to create divisions among allies about what was happening and how to respond – and thus break the Alliance politically, without firing a shot.13 This scenario reflects well-founded doubts about Alliance cohesion and unity. It does not reflect the reality of Russian strategy. An extensive search of Russian military writings produces no evidence of such considerations. Moreover, what we do know about Russian military thought suggests that a hybrid war with NATO would not make strategic sense from Moscow’s perspective. For the Russian military, the most significant threat in the Baltic region, particularly because of the strategically vulnerable Kaliningrad exclave, where the Russian Baltic Fleet is based, is the potential deployment of US forces and high-end capabilities. A Russian hybrid operation would give ample time for the US to do just that. So, in the time it took for Narva, the Russian-speaking Estonian border town, to be occupied by the little green men, the 101st Airborne Division could land in Tallinn and a US carrier group could set sail for the Gulf of Finland. Moreover, Moscow has options to prevent this scenario from materialising. For example, the army, with air support, could rapidly push from the Estonian border to the Baltic Sea, destroying all Estonian forces and denying the US access to the region before anyone in Washington or Brussels had the chance to navel gaze. One Russian analyst noted that it would take 30,000 NATO troops about a month to deploy to the Baltic region, while a Russian force of three times the size could be sent there in just 24 hours. He concluded that ‘while Europe’s top brass discuss and argue how to transit to the theater, and coordinate all of this with [the US], Warsaw, Riga, Tallinn and Vilnius would be transformed into a rubbish heap’.14 Some analysts have gone even further than discerning a doctrine and now claim that Russia is already conducting hybrid warfare on the West. As one recent report claimed, ‘The various diplomatic, economic, military and subversive measures that have been employed by Russia in the Baltic Region and increasingly in the Balkans, Black Sea and Mediterranean regions, could be interpreted as elements of a protracted campaign already underway.’15 The author thus equates hard-nosed – but commonplace – tactics to gain influence with subversion that represents a threat to national security. But there is a major difference between efforts to subvert a population against its government on the one hand, and the use of normal tools of statecraft to gain influence on the other.16 The former would be, of course, a real problem for NATO; fortunately, nothing like the subversion of eastern Ukraine is happening inside member states today. As for all the other unpleasant activities that Russia undertakes inside NATO and EU member states, such as funding political parties or developing media in local languages, these certainly do not merit the label ‘hybrid’, let alone ‘war’. After all, Western countries have been doing many of the same things inside of Russia for years. And no one considered those activities ‘elements of a protracted campaign already underway’. \* \* \* Three parallels between the developing conventional wisdom in Russia and the West on hybrid war emerge from the literature. Firstly, Russian strategists believe that the US is willing to risk conducting a limited, hybrid operation in Russia – that is, on the territory of a nuclear power – just as NATO strategists believe Russia is willing to risk the same on the territory of a nuclear alliance. Secondly, Russian analysts project well-founded fears about their country’s long-term political cohesion onto the West’s intentions. In other words, they know their political system is brittle, so therefore the Americans must be out to undermine it. In the same way, NATO analysts know there are divergences regarding threat perceptions inside the Alliance, so therefore Russia must be planning to take advantage of them. Finally, each side believes that Ukraine represents the other’s successful hybrid operation, and a potential precursor to such an operation being directed against it. Fortunately, on all three counts, the new conventional wisdom in both Russia and the West is wrong.

#### It doesn’t escalate

Heine Sørensen 19, Senior Lecturer at the Institute for Strategy at the Royal Danish Defence College, and Dorthe Bach Nyemann, Senior Lecturer at the Institute for Strategy, Royal Danish Defence College, Represented Denmark in the research Project entitled “Countering Hybrid Warfare I-II” Within the Framework of the Multinational Capability Development Campaign (MCDC), US Joint Forces Command, “Deterrence by Punishment as a Way of Countering Hybrid Threats – Why We Need To Go ‘Beyond Resilience’ in the Gray Zone”, Multinational Capability Development Campaign, March 2019, https://tinyurl.com/y6cko3at

The Flipside of Deterrence by Punishment – the Fear of Escalation One of the greatest reservations against communicating a willingness to take punitive actions concerns the risk of escalation and increased tension due to a more assertive or offensive posture. Yet when looking into possible responses – retaliation in cyberspace, for example – a number of “self-dampening” mechanisms appear to be in place that may be applicable to many types of responses.30 One example is the requirement to establish some level of attribution of aggression on which to base a response. As discussed above, while attribution is rarely impossible, it can be a time-consuming and technically-challenging endeavor. In a high-stakes scenario the time taken to get attribution as right as possible means there will be plenty of time to think twice about actions and consequences, and to lean on diplomatic measures in parallel. An example of a self-dampening mechanism related to the cyber domain is the large investment required to develop credible offensive capabilities. Moreover, an offensive cyber capability is a transitory tool31. The ability to access a computer system or network to cause harm or damage is only temporary and dependent on a very rapid and ongoing patching of vulnerabilities. At the same time, wielding the cyber instrument despite the downside of “burning” the capacity might have a de-escalatory effect by communicating capability and credibility to the opponent with a view to discouraging future hostile attacks. Targeting in any domain – including cyberspace – must also follow relevant rules, law and due-process which will self-limit the range of targets and actions available. A final “escalatory showstopper” is related to the challenge of identifying and developing targets of adequate strategic significance – not too much, not too little – to achieve the desired effect. Responding to hybrid aggression by applying “middle range” punitive actions that are proportionate to the aggression threatened or suffered will also self-limit the escalatory potential. It is unlikely to be in the interest of any hybrid aggressor to pursue an escalatory spiral above and beyond where they were looking to compete in the first place: on the hybrid level. Nevertheless, one way to mitigate the risk of escalation – while enhancing civilian oversight and interagency coordination – would be to establish rules of engagement for punitive actions on the hybrid level32 . This would provide decision-makers with common guidelines to pursue punitive actions that fall below the “use of force threshold”. Moreover, this could actually bolster the credibility of punitive actions by signaling to hybrid aggressors the intent to take pre-prepared punitive actions when deemed necessary: in other words, a “playbook” for countering hybrid threats.

#### No North Korean cyber attacks

Dr. James Andrew Lewis 17, Senior Vice President at the Center for Strategic and International Studies, Director of the Technology Policy Program, PhD from the University of Chicago, “The Likelihood of North Korean Cyber Attacks”, 9/7/2017, https://www.csis.org/analysis/likelihood-north-korean-cyber-attacks

Under what circumstances would it make sense for North Korea’s Kim regime to begin a war with the United States? The primary goal of any state is survival, and this is even more important for politically fragile regimes that provide immense benefit to the ruling family. An upper limit to North Korean activities is that, though it will use threats and coercive acts to pursue its larger policy goals, it will not do so at the expense of its own survival. There is some risk that Kim Jong-un could miscalculate when it comes to coercive acts. Shooting missiles over Guam would provoke a reaction, as would an inadvertent impact on Japanese territory of a missile intended to overfly it. But in general, behind the bluster, the Kim regime has been calculating and careful. This is the lens through which we should measure the risk of North Korea launching a cyber attack against the United States. North Korea is the least capable of our opponents when it comes to cyber attack. It uses cyber techniques for coercive diplomacy, for criminal activities to generate hard currency, and for disruptive actions in the South and against deployed U.S. forces. If war breaks out, the North might also consider cyber attacks against military or symbolic targets in the United States. However, short of armed conflict, disruptive actions here are unlikely. How disruptive a North Korean cyber attack would be depends on the victim’s weaknesses. North Korean successes depend on relatively basic techniques that exploit vulnerabilities in poorly defended systems. Though the North has used cyber attacks several times against South Korean banks and media outlets, and against Sony in the United States, none of those attacks caused physical destruction or casualties. To be fair, no cyber attack has ever caused casualties, and only three or four resulted in physical damage. North Korea, despite progress in developing its cyber-attack capabilities, does not possess the advanced skills needed to cause physical damage. What the North can do with cyber operations is disrupt data and online services. A 2011 cyber attack on a South Korean bank left customers unable to use ATMs or online services for several days. The action deleted customer accounts and tried to erase evidence of the attack from the bank’s computers. Similar attacks took place in 2013 against banks and media outlets in Seoul, with data erased and services disrupted. The 2014 attack on Sony Pictures also disrupted services and data and saw leaks of embarrassing e-mails. The most recent North Korean cyber incident used false credentials to steal $81 million from the Bangladesh Central Bank. While these count as successes, they may have also increased North Korea’s caution. If you think you are invisible and suddenly discover that you are not, it dampens your enthusiasm for crime. The ability of the United States to identify North Korea in the Sony incident probably led the North to revise upward the risk of cyber action against U.S. targets. We can run through one popular scenario to explore how North Korea might think about cyber attacks. Though it is unlikely that North Korea has the ability to cause blackouts in the United States, if it did have the capability and decided to use it, this would not reduce our ability to retaliate militarily. Blackouts do not produce catastrophe or military advantage. A cyber-induced blackout would, however, put the regime’s survival at risk—in diplomatic parlance, this is called poking a bear with a stick. In any event, the notion of cyber catastrophe is wildly exaggerated, reflecting a popular culture prone to exaggerating risk rather than seriously assessing an opponent’s capability and intent. North Korea uses cyber attacks to advance its policy agenda; none of its actions has been capricious or haphazard. Cyber attacks do not come out of the blue. They are not random acts (and they are not launched by groups with funny names) but are calculated to achieve either political or financial goals. A decision to launch a cyber attack would be made by Kim Jong-un, and he would consider this in the context of the larger efforts to manipulate decisionmakers and public opinion in the United States, Japan, and South Korea. An attack on critical infrastructure located in the domestic United States would be extremely provocative, and there are plenty of other provocative things the North can do that do not create existential risk for the Kim regime. Kim and his advisers probably know that China and Russia would look unfavorably on a cyber attack against the United States at this tense juncture, and while the North may be ready to ignore its patrons in some matters, starting an armed conflict with the United States is not one of them. It is commonplace to call Kim crazy, but his decisions are rational in the context of North Korea’s strategic culture. An attack on the United States that the North believes is likely to be detected, that will not produce significant harm, and that could generate a damaging response is unattractive. The goal is to manipulate the United States and its North Asian allies without provoking war, and cyber attacks on the U.S. homeland, catastrophic or otherwise, run counter to this